Université de Montréal

Méthodes pour la réduction d'attaques actives à passives en cryptographie quantique

par
Philippe Lamontagne

Faculté des arts et sciences
Département d'informatique et de recherche opérationnelle

Thèse présentée en vue de l'obtention du grade de
Philosophiæ Doctor (Ph.D.) en informatique

Décembre 2017

Résumé

La mécanique quantique offre un avantage indéniable sur la mécanique classique pour la réalisation de diverses tâches cryptographiques. Cependant, elle ouvre également la voie à des attaques complexes qui compliquent l'analyse des protocoles cryptographiques. Ainsi, les cryptographes sont constamment à la recherche de nouveaux outils qui permettent de simplifier les preuves. Dans cette thèse, nous introduisons de nouvelles techniques qui permettent de simplifier l'analyse de protocoles cryptographiques quantiques et nous en démontrons l'utilité par quelques exemples d'applications. Nos techniques permettent de montrer que, sous certaines conditions, la sûreté d'un protocole cryptographique contre une attaque qui respecte plus ou moins le protocole (passive) est une condition suffisante pour montrer la sûreté contre une attaque qui peut dévier du protocole (active).

Nous montrons d'abord que la sécurité d'un protocole quantique contre les adversaires sans mémoire quantique implique sa sécurité contre les adversaires disposant d'une certaine quantité de mémoire. Cette technique trouve son utilité dans le fait que les attaques ayant accès à une mémoire quantique sont généralement bien plus difficiles à analyser que celles sans mémoire. Nous introduisons ensuite la certification d'états mixtes : étant donné un registre quantique composé de n qubits, nous montrons qu'il est possible de s'assurer que ce registre est près de n copies d'une même matrice de densité φ. Cet outil offre un cadre général pour analyser une situation commune en cryptographie quantique où une source non fiable fournit un état quantique et on veut s'assurer que l'état fourni par cette source est le bon.

Ces résultats ont permis de contribuer aux connaissances en cryptographie quantique par les avancées suivantes. D'abord, nous résolvons deux problèmes ouverts, l'un concernant la puissance cryptographique de la primitive *cut-and-choose* à un bit, et l'autre concernant la sûreté du protocole de mise en gage BCJL. Dans les deux cas, notre relation entre les adversaires quantiques et les adversaires sans mémoire joue un rôle central. Par la suite, nous introduisons une nouvelle tâche cryptographique où deux participants veulent générer une chaine de bits commune quasi uniformément distribuée, et ce même si l'un des participants est malhonnête. Nous présentons un protocole quantique qui surpasse tout protocole classique pour cette tâche.

Mots clés cryptographie quantique, mise en gage, cut-and-choose, tirage d'une pièce, échantillonnage quantique, certification d'états mixtes, attaques (non) adaptives, modèle à mémoire bornée/bruitée

Abstract

Quantum mechanics offers an undeniable advantage over classical mechanics for conceiving protocols for cryptographic tasks. However, it also enables complex attacks that make quantum protocols hard to analyse and cryptographers are thus always looking for new tools to simplify proofs. In this thesis, we introduce new techniques that simplify the analysis of quantum cryptographic protocols and we showcase their usefulness with some applications. Our techniques are used to show that, under certain conditions, the security of a protocol against an attacker that more or less follows the honest behaviour (passive) is a sufficient condition to show the security against arbitrary attacks (active).

We first demonstrate a general technique for reducing the security of a quantum protocol against an attacker with some amount of quantum memory to its security against an attacker with no quantum memory at all. This technique is especially useful due to the fact that attacks that have access to a quantum memory are notoriously difficult to analyse. We then introduce a second technique for certifying that a quantum population is close to a given mixed reference state : given n quantum registers, it is possible to make sure that the state of these n registers is close to $\varphi^{\otimes n}$ for some mixed state φ. This technique offers a general framework for analysing a common situation in quantum cryptography where we want to certify that a state prepared by a distrusted source is close to the honest state.

Both our techniques allowed us to contribute to the advancement of knowledge in quantum cryptography. Our first result is the main tool used to solve two open problems : the first concerning the cryptographic power of the one bit *cut-and-choose* primitive, and the second concerning the security of the BCJL bit commitment protocol. Our second technique is used to prove the security of a protocol that implements the task of producing a common random bit string that is almost uniformly distributed, even if one of the parties is dishonest. Our protocol outperforms any classical protocol for this task.

Keywords quantum cryptography, bit commitment, cut-and-choose, coin-tossing, quantum sampling, mixed state certification, (non-)adaptive attacks, bounded/noisy storage model

Table des matières

Table des figures

Notation

Symbole	Description	Page
$:=$	Définition	10
$f \circ g$	Composition des deux applications f et g : $f \circ g(x) := f(g(x))$	
$\text{supp}(A)$	Support de l'opérateur A	13
$d(x, y)$	Distance de Hamming entre x et y	13
$wt(x)$	Poid de Hamming de x	13
$w(x)$	Poid de Hamming relatif de $x \in \{0,1\}^n$: $wt(x)/n$	13
$\in_R$ ou $\subset_R$	Élément ou ensemble choisi aléatoirement de manière uniforme	10
$\mathbb{1}_{\mathcal{X}}$	En tant qu'opérateur sur $\mathcal{X}$: identité sur $\mathcal{X}$. En tant qu'opérateur sur $\mathcal{Y} \supseteq \mathcal{X}$: projecteur sur $\mathcal{X}$.	13
$[n]$	L'ensemble $\{1, \ldots, n\}$.	10
$\bar{X}$	Le complément de l'ensemble X.	10
$\lvert X \rvert$	Cardinalité de l'ensemble X	10
0^n	Chaine de bits composée de n zéros	10
x_t	Éléments de $x \in \Sigma^n$ restreints aux positions dans $t \subset [n]$.	10
$B^\delta(x)$	Sphère de Hamming de rayon δn autours de $x \in \{0,1\}^n$.	10
$h(\cdot)$	Fonction d'entropie binaire.	10
$\text{negl}(n)$	Fonction négligeable en n	11
$\mathcal{X}, \mathcal{Y}, \mathcal{Z}$	Espaces de Hilbert	12
$\dim(\mathcal{X})$	Dimension de l'espace $\mathcal{X}$	12
A^*	Transposée conjuguée de A	12
$\lVert \lvert u \rangle \rVert$	Norme euclidienne du vecteur $\lvert u \rangle$	12
$L(\mathcal{X}, \mathcal{Y})$	Ensemble des opérateurs linéaire de $\mathcal{X}$ vers $\mathcal{Y}$.	13
$L(\mathcal{X})$	$L(\mathcal{X}, \mathcal{X})$	
$A_{\mathcal{X} \to \mathcal{Y}}$	Opérateur dans $L(\mathcal{X}, \mathcal{Y})$	13
$U(\mathcal{X}, \mathcal{Y})$	Ensemble des isométries de $\mathcal{X}$ vers $\mathcal{Y}$.	13

$\lvert u\rangle\langle u\rvert$	Opérateur de projection sur le sous-espace engendré par le vecteur $\lvert u\rangle$.	
$\mathbb{P}, \mathbb{Q}, \ldots$	Opérateur de projection	
$\lVert A\rVert_1$	Norme de trace de l'opérateur A	17
$\lVert A\rVert_\infty$	Norme spectrale de l'opérateur A	17
$\mathsf{A}, \mathsf{B}, \mathsf{C}, \ldots$	Registres quantiques	17
A^n	Registre composé des n registres identiques $\mathsf{A}_1, \ldots, \mathsf{A}_n$	
$\mathcal{H}_\mathsf{A}$	Espace de Hilbert associé au registre A	
$\mathcal{D}(\mathcal{X})$	Ensemble des opérateurs de densité sur l'espace $\mathcal{X}$.	18
$\mathcal{D}_\leq(\mathcal{X})$	Ensemble des opérateurs $\rho \in L(\mathcal{X})$ tels que $\rho \geq 0$ et $\mathrm{tr}(\rho) \leq 1$.	18
$\mathcal{S}(\mathcal{X})$	Ensemble des états purs sur l'espace $\mathcal{X}$	18
$A_{\mathsf{A}\to\mathsf{B}}$	Opérateur dans $L(\mathcal{H}_\mathsf{A}, \mathcal{H}_\mathsf{B})$	20
ρ^E	État conditionné sur l'évènement E.	22
$\mathrm{span}\{\lvert u_1\rangle, \ldots, \lvert u_n\rangle\}$	Sous-espace engendré par les vecteurs $\lvert u_1\rangle, \ldots, \lvert u_n\rangle$	12
$A^{\otimes n}$ pour $n \in \mathbb{N}$	$\underbrace{A \otimes \cdots \otimes A}_{n \text{ fois}}$	15
$A^{\otimes\theta}$ pour $\theta \in \{0,1\}^n$	$\bigotimes_{i=1}^n A^{\theta_i}$ et où $A^0 := \mathbb{1}$ et $A^1 := A$	15
$D(\rho, \sigma)$	Distance de trace entre les matrices de densité ρ et σ	22
$F(\rho, \sigma)$	Fidélité entre les matrices de densité ρ et σ	23
$\Delta_r(\lvert\psi\rangle)$	Sphère de Hamming quantique de rayon r autour de $\lvert\psi\rangle$	37
OT	Primitive cryptographique	25
$\mathcal{F}_{\mathrm{OT}}$	Fonctionnalité idéale de la primitive OT	25
Π_{OT}	Protocole pour la primitive OT	25
$\Pi^\mathcal{F}$	Protocole dans le modèle $\mathcal{F}$-hybride	28
$\sqsubseteq$	Réduction cryptographique	29
$\mathrm{H}_\infty(\rho_\mathsf{A})$	Min-entropie de l'état ρ_A	31
$\mathrm{H}_0(\rho_\mathsf{A})$	Max-entropie de l'état ρ_A	31
$\mathcal{S}_n$	Groupe des permutations de n éléments	34
$\mathrm{Sym}^n(\mathcal{H})$	Sous-espace symétrique de $\mathcal{H}^{\otimes n}$	34

Abbréviations

OLCC	Opérations Locales et Communication Classique
CPTP	Super-opérateur complètement positif qui préserve la trace
CPTN	Super-opérateur complètement positif qui n'augmente pas la trace
BCJL	Brassard, Crépeau, Jozsa et Langlois
UC	Universellement Composable
EPR	Einstein, Podolsky et Rosen
POVM	Mesure à opérateurs positifs
i.i.d.	indépendamment et identiquement distribué
s.p.d.g.	sans perte de généralité

Remerciements

Je remercie d'abord mes parents pour m'avoir encouragé tout au long de mes études et de m'avoir fourni un environnement privilégié sans lequel je n'aurais pu me rendre aussi loin dans les études supérieures.

Je remercie Karelle Dupuis pour sa confiance, pour son soutien, pour ses encouragements, mais surtout pour son amour.

Je remercie Michael Blondin, Mathieu Janelle Gravel et Simon Lamontagne de m'avoir sorti de la routine, pour m'avoir donné une vie sociale et pour m'avoir écouté me plaindre à d'innombrables reprises. Je remercie spécialement Michael de m'avoir servi de modèle tout au long de nos parcours semblables.

Je remercie mon directeur Louis Salvail de m'avoir aidé à terminer cette thèse, pour son mentorat et pour le support financier sans lequel mon doctorat n'aurait pas eu lieu. Je remercie également mes coauteurs Frédéric Dupuis et Serge Fehr pour le temps et la patience qu'ils ont investis malgré les nombreuses embuches.

Chapitre 1

Introduction

1.1 Qu'est-ce que la cryptographie ?

La cryptographie, dans sa version traditionnelle, décrit l'ensemble des techniques pour la conception et l'analyse de codes que nous appelons *chiffres* qui permettent la transmission secrète de messages. Un chiffre est un encodage de l'information qui permet à deux interlocuteurs d'échanger des messages de manière privée, même si une personne à l'oreille indiscrète tente d'épier le contenu de leur conversation. Pour que cette tâche soit possible il faut que les interlocuteurs disposent d'un certain avantage sur l'épieur sous la forme d'une *clé secrète* — information connue seulement par les interlocuteurs. Cette clé sert à chiffrer et à déchiffrer les messages à transmettre.

La cryptographie a un long historique avec des chiffres qui remontent au moins aussi loin que Jules César [KL14] qui utilisait un chiffrement par substitution pour chiffrer ses messages destinés à ses généraux. Le plus simple de ces chiffres consiste en un simple décalage des lettres de l'alphabet. Par exemple pour un décalage de 3, A devient D, B devient E, etc. Ainsi, le message `Attaquez a l'aube`, chiffré avec la clé $k = 3$, deviendra le chiffre `Dwwdtxhc d o'dxeh`. Une personne connaissant la clé peut inverser cette transformation et retrouver le message original. Bien sûr, cette technique de chiffrement n'est aucunement sûre car il suffit d'essayer les 26 clés possibles pour trouver le message qui est syntaxiquement correct pour, par exemple, le français.

L'attaque exhibée ci-dessus démontre bien l'importance d'avoir un espace de clés de taille suffisante pour qu'il ne soit pas possible de simplement deviner la clé. C'est Claude Shannon qui, dans les années 1940 [Sha49], établit les bases de la cryptographie moderne et qui montra entre autres choses que pour

qu'un chiffre soit 100% sûr en général, la clé doit être aussi longue que le message qu'elle chiffre. La cryptographie moderne repose sur trois principes fondamentaux. D'abord, on doit énoncer de manière claire et précise une *définition de sécurité*. Lorsqu'une construction cryptographique repose sur des *hypothèses non prouvées*, celles-ci doivent être énoncées de manière précise et l'utilisation de telles hypothèses devrait être minimale. Finalement, chaque construction doit être accompagnée d'une preuve rigoureuse qu'elle satisfait une définition de sécurité énoncée selon le premier principe, à partir d'hypothèses qui satisfont le deuxième principe (si de telles hypothèses sont nécessaires).

La cryptographie moderne s'intéresse à l'ensemble des problèmes qui concernent la confidentialité et l'authenticité d'information sensible. La sous-section suivante présente un tel problème où deux participants veulent calculer une fonction conjointe de leurs informations sensibles respectives.

1.1.1 L'évaluation sûre à deux participants

Considérons le problème suivant : deux millionnaires désirent savoir lequel d'entre eux est le plus riche, mais aucun n'est prêt à dévoiler le montant de sa fortune à l'autre. Comment peuvent-ils déterminer lequel possède le plus ? Une manière évidente serait de montrer leur compte bancaire à un arbitre en qui ils ont tous deux confiance et cet arbitre leur indiquerait qui est le plus riche, sans dévoiler quoi que ce soit d'autre sur les fortunes respectives des deux millionnaires. Dans une situation normale, un tel arbitre n'est que rarement disponible. Comment alors les deux millionnaires peuvent-ils, par des échanges successifs de messages, établir lequel est le plus riche sans dévoiler trop d'information ? C'est à ce genre de question que s'intéresse le sous-domaine de la cryptographie nommé *évaluation sûre de fonctionnalités*. Grâce à un protocole cryptographique qu'exécuteront les deux millionnaires, on veut simuler l'arbitre par l'envoi successif de messages.

En général, cette tâche implique deux participants que nous nommerons Alice et Bob et qui détiennent chacun une certaine information (respectivement x et y). Ils veulent calculer une fonction conjointe de leurs informations : $f(x, y) = (f_1(x, y), f_2(x, y))$ où Alice reçoit $f_1(x, y)$ et Bob reçoit $f_2(x, y)$. Comme dans l'exemple précédent, Alice ne doit rien apprendre sur y autre que ce qu'elle peut déduire à partir de x et $f_1(x, y)$, et de même pour Bob. Ils tenteront donc, par l'usage d'un protocole biparti, de simuler l'arbitre de l'exemple précédent qu'on représente par une *fonctionnalité idéale*, c'est-à-dire une boîte noire à laquelle Alice donne x et Bob donne y et qui retourne $f_1(x, y)$ et $f_2(x, y)$ à Alice et à Bob, respectivement.

C'est un fait bien connu que l'évaluation sûre de fonctions est une tâche impossible sans hypothèses. Ainsi une question naturelle est : quelles sont les hypothèses minimales qui permettent cette tâche ? Une réponse à cette question est de trouver la *primitive cryptographique*, c'est-à-dire la fonction f, la plus simple

telle que si on sait évaluer f de manière sûre, alors on peut l'utiliser comme bloc de construction pour évaluer n'importe quelle autre fonction g. Si on sait construire un protocole pour f à partir d'hypothèses calculatoires ou physiques, on peut alors évaluer de manière sûre toute fonction g à partir de cette même hypothèse. C'est sur ce type de problème que porte la présente thèse.

1.2 La mécanique quantique

La mécanique quantique vit le jour au début du 20$^{\text{e}}$ siècle avec les travaux de Planck, Einstein, Bohr, Schrödinger, Heisenberg, Pauli, Born et autres. Elle décrit le comportement des particules à l'échelle atomique et subatomique. Il existe des ouvrages entiers dédiés à la mécanique quantique et à ses interprétations, mais nous nous contenterons dans cette section d'en donner une certaine image et d'exhiber ses propriétés principales pour le traitement de l'*information quantique*.

De la même manière que l'information classique est contenue dans des registres mémoires pour des fins de traitements de l'information, nous allons supposer que l'information quantique que nous traitons réside dans des *registres quantiques* de taille finie. Nous faisons abstraction de la réalisation physique de ces registres tout comme nous faisons abstraction de la manière dont l'information classique est enregistrée lorsque nous traitons cette dernière. Tout comme les registres classiques ont une certaine capacité fixe (par exemple un registre de 64 bits), les registres quantiques ont une capacité fixe de stockage d'information pour une mesure de quantité d'information quantique que nous introduirons sous peu — le *qubit* — qui correspond à l'analogue quantique du bit classique.

Plusieurs propriétés uniques à la mécanique quantique la rendent intéressante pour des fins de traitement de l'information. Par exemple, un qubit peut être dans deux états *de base* $|0\rangle$ et $|1\rangle$, mais peut aussi être dans une *superposition* de ces deux états,

$$\alpha|0\rangle + \beta|1\rangle$$

où $\alpha, \beta \in \mathbb{C}$ sont des *amplitudes* qui satisfont $|\alpha|^2 + |\beta|^2 = 1$. Du principe de la superposition découle celui de *l'intrication*. L'état de deux qubits

$$\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

est l'exemple canonique d'un état intriqué. L'intrication est probablement la propriété la plus surprenante et contre-intuitive de la mécanique quantique : c'est une corrélation bien plus forte que tout ce qui est possible classiquement et permet des tâches de traitement et de transmission de l'information intéressantes. La *téléportation quantique* [BBC$^+$93] et le *codage superdense* [BW92] sont deux exemples importants parmi les multiples applications de l'intrication au traitement de l'information sur de longues distances.

Une autre particularité de la mécanique quantique est qu'il n'est pas possible en général d'apprendre avec certitude l'état d'un qubit. En effet, pour extraire de l'information classique (macroscopique) d'un qubit, on doit le *mesurer*. Si un qubit est dans l'état $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ et qu'on le mesure (dans la base $\{|0\rangle, |1\rangle\}$) on obtiendra $|0\rangle$ avec probabilité $|\alpha|^2$ et $|1\rangle$ avec probabilité $|\beta|^2$. Cette opération *perturbe* le qubit : si on observe $|0\rangle$, alors l'état du qubit devient $|0\rangle$ et de même pour $|1\rangle$. Ceci fait en sorte que si nous disposons d'une seule copie de $|\phi\rangle$, il nous est impossible d'apprendre avec précision la valeur de α ou β. Cette *incertitude* sur l'état d'un système quantique, de pair avec l'impossibilité de copier l'information quantique, sont des propriétés de la mécanique quantique qui ont des implications importantes pour la cryptographie.

1.2.1 Pourquoi la cryptographie quantique ?

Comme mentionné plus haut, la mécanique quantique offre des propriétés intéressantes pour certaines tâches de traitement de l'information, et en particulier pour la cryptographie. Plusieurs propriétés de la mécanique quantique ont des conséquences importantes pour la cryptographie : l'impact le plus grave qu'aura la venue de l'ordinateur quantique sur nos vies est sans aucun doute l'algorithme de Shor [Sho94], un algorithme quantique efficace pour résoudre le problème de la factorisation de grands nombres et le problème de l'extraction du logarithme discret. Ces problèmes, supposés difficiles à résoudre sur un ordinateur classique, sont les hypothèses fondatrices de la cryptographie à clé publique qui a permis l'évolution de l'internet et du commerce en ligne tels qu'on les connait.

Mais au-delà de sonner le glas des infrastructures cryptographiques existantes, la mécanique quantique offre aussi de nouvelles possibilités cryptographiques. La tâche cryptographique quantique la plus célèbre est certainement la *distribution de clé quantique*, inventée par Charles Bennett et Gilles Brassard au début des années 1980 [BB83, BB84]. La distribution de clé quantique offre une solution quantique au problème d'établissement d'une clé secrète entre deux participants qui communiquent par un canal classique *authentifié*. Alors que les solutions classiques existantes utilisent les hypothèses calculatoires défaites par l'algorithme de Shor, la distribution de clé quantique utilise un canal quantique non sûr en plus du canal classique authentifié pour l'établissement d'une clé secrète. La propriété de la mécanique quantique qui rend cette tâche possible est le fait qu'observer un système quantique pour gagner de l'information sur son état perturbe celui-ci. Ainsi un adversaire qui tente de deviner la clé en épiant le canal quantique perturbe l'information d'une manière détectable par les deux participants.

Les nouvelles possibilités cryptographiques offertes par la mécanique quantique ne s'arrêtent pas à l'établissement de clé, le quantique offre un avantage démontrable sur le classique pour l'évaluation sûre de fonctions : ce problème devient possible avec des hypothèses strictement plus faibles lorsqu'on exploite

les propriétés uniques à la mécanique quantique. Cette thèse porte justement sur les implications de la mécanique quantique pour l'évaluation sûre à deux participants.

1.2.2 Bref historique de la cryptographie quantique

La première proposition d'utiliser les propriétés quantiques de la matière à des fins cryptographiques remonte aux travaux de Stephen Wiesner [Wie83] à partir de 1968. Bien qu'ils ne furent publiés qu'en 1983, après que des avancées en cryptographie permettent d'en apprécier la valeur, ces travaux étaient en avance sur leur temps. Wiesner proposa d'utiliser le principe d'incertitude de la mécanique quantique pour encoder deux messages dans un état quantique de manière à ce que seul un des deux messages puisse être récupéré avec certitude. Il s'agit là du premier protocole quantique pour une variante [1] de la primitive cryptographique OT [2], plusieurs années avant que cette primitive ne soit introduite par Michael Rabin [Rab81]. Nous savons maintenant que cette tâche n'est pas plus réalisable dans le monde quantique que dans le monde classique sans hypothèse supplémentaire, mais Wiesner n'affirmait pas le contraire. Dans ce même article, il démontre qu'un receveur disposant d'une technologie assez sophistiquée pourrait tricher le protocole. Cela n'empêche que le protocole de Wiesner exploitait une certaine *asymétrie* entre comportements adversariel et honnête qui sera reprise dans plusieurs constructions cryptographiques modernes : l'attaque de l'adversaire nécessite une technologie (quantique) grandement supérieure à celle suffisante pour un comportement honnête.

La parution scientifique qui inventa le terme « cryptographie quantique » fut un papier par Bennett, Brassard, Breidbart et Wiesner [BBBW83] qui reprirent les idées de Wiesner et les présentèrent d'une manière appréciable par la communauté cryptographique de l'époque. Par contre, l'étude de la cryptographie quantique demeura plutôt marginale jusqu'à l'invention de la distribution de clé quantique par Bennett et Brassard [BB83, BB84] et de la démonstration de la faisabilité physique de leur protocole [BB89, BBB$^+$92] qui attira l'attention des communautés de recherche en cryptographie et en physique. Il existe aujourd'hui un riche domaine de recherche sur la distribution de clé quantique, mais comme ces résultats ne concernent pas l'évaluation sûre à deux participants, le sujet de cette thèse, nous n'irons pas plus loin dans cette direction.

La cryptographie quantique ne se limite pas à la distribution de clé quantique, tout comme la cryptographie en général ne se limite pas à la communication secrète. Dans un papier paru en 1993, Brassard, Crépeau, Jozsa et Langlois [BCJL93] construisirent un protocole quantique basé sur les idées de Wiesner et les techniques employées dans [BB84] pour la primitive cryptographique de *mise en gage*, une primitive

1. On sait maintenant que toutes les variantes de cette primitive sont équivalentes [Cré88].
2. De l'anglais *oblivious transfer*.

permettant à un participant de s'engager à une certaine valeur secrète et ainsi avoir la possibilité de dévoiler cette valeur dans le futur, mais sans pouvoir la modifier. Ce protocole était accompagné d'une preuve qu'il était inconditionnellement sûr, cependant cette preuve ne prenait pas en compte un nouveau type d'attaque permis par la mécanique quantique, les attaques *par purification* qui exploitent les propriétés de l'intrication [May96]. Le protocole de [BCJL93], s'il était sûr, aurait impliqué que la mécanique quantique est une hypothèse suffisante pour accomplir toute tâche cryptographique, car durant la même période on montra [BBCS91] qu'il est possible de construire la primitive OT à partir d'un protocole de mise en gage dans le monde quantique, et il était déjà connu que OT était une hypothèse suffisante pour l'évaluation sûre de fonctions [Kil88]. Le résultat est tout de même intéressant en soi, car classiquement, la mise en gage est strictement plus faible que OT sans hypothèses supplémentaires [PR08].

L'attaque mentionnée au paragraphe précédent contre le protocole de mise en gage de [BCJL93] se généralise pour montrer que la mise en gage quantique est impossible. Cette attaque générale fut découverte indépendamment par Dominic Mayers [May97] et Lo et Chau [LC98]. Bien que ces résultats montrent que la tâche de l'évaluation sûre de fonctionnalités est impossible en général dans le monde quantique sans hypothèse supplémentaire (puisque la mise en gage en est un cas spécial), plusieurs travaux portent tout de même sur des résultats d'impossibilité *explicites* qui présentent des attaques générales pour ce type de problème [Lo97, Col07, BCS12].

Les attaques présentées dans les résultats ci-dessus requièrent des capacités technologiques considérables pour être réalisées par un adversaire quantique. Elles demandent en général de préserver l'information quantique de manière cohérente pendant l'exécution du protocole, une prouesse qui est loin d'être réalisable avec la technologie actuelle. Il devient alors très naturel d'utiliser comme hypothèse cryptographique le fait que l'adversaire ne peut garder qu'une petite quantité d'information quantique en mémoire. Cette hypothèse est en effet suffisante pour l'évaluation sûre de fonctionnalités [DFSS08, DFSS07, Sch07] : un adversaire qui ne peut pas enregistrer plus qu'une certaine fraction (généralement $\frac{1}{2}$ ou $\frac{1}{4}$) de l'information quantique échangée ne peut pas tricher le protocole. Cette hypothèse se généralise également au cas où la mémoire de l'adversaire est *bruitée* [WST08, STW09, WCSL10, Sch10, KWW12] où une certaine perturbation est ajoutée à la mémoire de l'adversaire, ce qui correspond à l'interaction d'un système quantique avec son environnement. Ces hypothèses sont d'autant plus intéressantes que la plupart des protocoles quantiques basés sur celles-ci ne demandent pas aux participants honnêtes de posséder de mémoire quantique.

1.3 Structure de la thèse et aperçu des contributions

Le chapitre 2 introduit les notions mathématiques nécessaires à la compréhension de ce document. Une certaine connaissance de base des mathématiques est supposée, par exemple la théorie des probabilités et l'algèbre linéaire. On suppose également que le lecteur dispose de connaissances de base en informatique. Les chapitres centraux (chapitres 3 et 4) présentent les travaux de recherche effectués dans le cadre de cette thèse. Finalement, le chapitre 5 conclut en résumant les contributions de cette thèse. Cette thèse dispose également d'une annexe qui contient quelques preuves trop longues pour trouver place dans le document principal.

1.3.1 Contributions

Cette thèse considère les protocoles cryptographiques quantiques et les attaques contre ces protocoles. Comme l'analyse directe de ces protocoles n'est pas toujours simple, à cause de la complexité des attaques, il est utile d'avoir des outils permettant d'en simplifier l'analyse. Les contributions principales de cette thèse sont de tels outils de preuve. Nous présentons deux résultats qui permettent, dans certaines situations, de réduire la sûreté d'un protocole contre un adversaire arbitraire (actif) à sa sûreté contre un adversaire qui dévie peu du comportement honnête (passif). Comme il est habituellement plus facile de montrer la sûreté contre les adversaires passifs, nos outils simplifient grandement l'analyse des protocoles auxquels ils s'appliquent.

Nous montrons d'abord un cadre général pour le traitement de l'information auxiliaire, soit l'information qu'acquiert l'adversaire durant le protocole et qui l'aide dans son attaque. Nous montrons que dans certaines situations, l'adversaire détenant de l'information auxiliaire (actif) se réduit à un adversaire n'en ayant pas (passif). Ensuite, nous montrons qu'il est possible de s'assurer qu'une population de registres quantiques préparés par un adversaire est près d'un certain état de prédilection. Nous montrons que tout adversaire qui dévie de manière trop importante du comportement honnête (passif) est détecté avec très grande probabilité.

Dans chacun des cas, nous illustrons l'utilité de nos résultats par leur application à des protocoles cryptographiques — nouveaux ou existants — où nos outils jouent un rôle central dans les preuves de sûreté.

Traitement général de l'information auxiliaire quantique. Le chapitre 3 présente les travaux de la première partie de cette thèse. Ces travaux ont été effectués en collaboration avec Louis Salvail, Frédéric Dupuis et Serge Fehr. Ils ont été publiés dans les actes de conférence de CRYPTO 2016 [DFLS16a] et

ont également été présentés à la conférence QCrypt 2016 [DFLS16b]. Ces travaux étudient l'évaluation sûre à deux participants dans le monde quantique et plus particulièrement une situation fréquente qui survient lors de l'analyse de protocoles quantiques où l'adversaire acquiert de *l'information auxiliaire* qui l'aide dans son attaque contre le protocole. On dit d'un adversaire qui dispose d'une telle information qu'il est *adapté*. Lorsque cette information auxiliaire est *quantique*, il devient beaucoup plus difficile de déterminer l'avantage que confère cette information à l'adversaire adapté. Les travaux présentés au chapitre 3 introduisent l'équivalent quantique de la relation

$$P_{\text{succ}}^{\text{A}} \leq 2^n P_{\text{succ}}^{\text{NA}} \tag{1.1}$$

où $P_{\text{succ}}^{\text{A}}$ (respectivement $P_{\text{succ}}^{\text{NA}}$) représente la probabilité de succès de l'attaque de l'adversaire adapté (respectivement non-adapté), où n est la taille de l'information auxiliaire.

Les relations du type de (1.1) sont particulièrement utiles dans un contexte quantique où il est généralement plus difficile de déterminer l'avantage que donne l'information auxiliaire quantique à l'adversaire, à cause de la complexité et de la puissance des attaques qui exploitent l'intrication. Les relations de ce type offrent un outil de preuve non trivial dans la mesure où la taille de l'information auxiliaire n peut être contrôlée et où on peut borner $P_{\text{succ}}^{\text{NA}}$ par une quantité négligeable, ce qui est généralement plus facile lorsque l'adversaire ne dispose pas d'information auxiliaire.

La pertinence de la relation (1.1) est ensuite établie en l'utilisant comme outil principal pour résoudre deux problèmes ouverts en cryptographie quantique. Le premier est un problème énoncé dans [FKS+13] qui concerne la puissance cryptographique de la primitive 1CC, décrite à la section 2.4, dans un contexte quantique. L'importance de cette question réside dans le fait qu'elle était la pièce manquante dans une classification des primitives cryptographiques dans le monde quantique. Nous montrons que 1CC appartient à la classe des primitives les plus puissantes, en utilisant la relation (1.1) pour simplifier notre argument. La deuxième question ouverte que nous considérons concerne la sûreté du protocole de mise en gage quantique présenté dans [BCJL93]. Comme mentionné à la section précédente, ce protocole n'est pas sûr sans hypothèses, mais sa sûreté n'avait jusqu'à présent pas été revisitée. Nous montrons que sous certaines hypothèses sur les capacités quantiques de l'adversaire, ce protocole est sûr. La relation (1.1) joue encore un rôle central dans la preuve de sécurité.

Échantillonnage quantique d'états de référence mixtes. Le chapitre 4 présente la deuxième partie des travaux du doctorat qui concernent *l'échantillonnage quantique*. Ces travaux, réalisés en collaboration avec Louis Salvail, Frédéric Dupuis et Serge Fehr [DFLS17], étudient l'échantillonnage statistique d'une population quantique (par exemple une population de qubits). Cette tâche est étudiée dans [BF10] pour le cas d'états de référence *purs*. Par exemple, si on veut vérifier que l'état de n qubits est *près* d'un état

de la forme $|0\rangle^{\otimes n}$, à quelques erreurs près, on mesurera un sous-ensemble aléatoire des qubits pour vérifier qu'ils sont dans l'état $|0\rangle$. On dit alors que $|0\rangle$ est *l'état de référence*. Les résultats de [BF10] ne nous disent toutefois rien sur la manière de s'y prendre si l'état de référence est sous la forme la plus générale, c'est-à-dire un état mixte.

Dans le chapitre 4, nous introduisons une procédure pour échantillonner une population quantique avec un état de référence mixte : nous montrons comment un échantillonneur peut vérifier qu'un registre est dans l'état $\varphi^{\otimes n}$ s'il a accès à un prouveur qui peut lui fournir des purifications de ses registres sur demande. Cette tâche est contre-intuitive ; dans le cas classique, elle correspond à vérifier qu'une chaine de bits a été générée selon une certaine distribution de probabilité. Ainsi, une contribution de ce travail est de définir ce à quoi on s'attend d'une telle tâche dans un contexte adversariel où le prouveur est malhonnête.

Notre contribution principale de ces travaux est l'introduction d'un modèle général pour la description et l'analyse de protocoles d'échantillonnage d'états mixtes dans un contexte adversariel. Nous montrons que n'importe quelle procédure d'échantillonnage qui peut être représentée sous une certaine forme et qui satisfait certaines propriétés peut être montrée sûre dans notre modèle. Une conséquence importante de cette généralité est que la plupart des résultats d'échantillonnage quantiques précédemment considérés peuvent être analysés dans notre modèle.

Nous appliquons cette nouvelle technique d'échantillonnage au problème de « tirage d'une pièce par téléphone ». Plus précisément, nous montrons comment le fait de tirer plusieurs pièces en même temps permet en quelque sorte « d'outrepasser » la preuve d'impossibilité du tirage par téléphone. Plus précisément, nous introduisons une nouvelle tâche cryptographique, soit la génération sûre d'aléa partagé où deux participants veulent produire une chaine commune $x \in \{0,1\}^n$ dont la distribution de probabilité est *presque* uniforme.

Chapitre 2

Notions préliminaires

2.1 Notation

Dans cette section, nous introduisons en rafale plusieurs éléments de la notation qui sera utilisée au courant de cette thèse. Une référence rapide à cette notation et à celle qui sera introduite plus loin dans ce chapitre se trouve au début du document en page ix. Au cours du document, et spécialement dans ce chapitre, nous utilisons la notation « := » lorsqu'il s'agit d'une égalité qui sert de définition.

Soit $\mathbb{N} := \{1, 2, 3, \ldots\}$ l'ensemble des entiers positifs. On définit $[a, b] := \{a, \ldots, b\}$ pour $a \leq b$, $a, b \in \mathbb{N}$. En particulier, $[n] := \{1, \ldots, n\}$ pour $n \in \mathbb{N}$. Soit Y un ensemble fini, pour n'importe quel sous-ensemble $X \subseteq Y$, $\bar{X}$ représente le complément de X dans Y, c'est-à-dire $\bar{X} = Y \setminus X$. La cardinalité d'un ensemble X est notée $|X|$. Pour un ensemble X, on écrit $x \in_R X$ (respectivement $x \subseteq_R X$) pour désigner que x est un élément (respectivement un sous-ensemble) de X choisi aléatoirement selon la distribution uniforme.

Pour une chaine binaire $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ et un sous-ensemble $t = \{t_1, \ldots t_k\} \subseteq [n]$, on écrit x_t pour la chaine $x_t = (x_{t_1}, \ldots, x_{t_k}) \in \{0,1\}^{|t|}$. En général, on omet les parenthèses et les virgules et on écrit simplement $x = x_1 \ldots x_n \in \{0,1\}^n$. La chaine binaire composée de n zéros est représentée par 0^n. La *distance de Hamming* entre deux chaines binaires $x, y \in \{0,1\}^n$ est définie par $d(x, y) := \sum_{i=1}^{n} x_i \oplus y_i$. Le *poids de Hamming* d'une chaine $x \in \{0,1\}^n$ est $wt(x) := d(x, 0^n)$, autrement dit, c'est le nombre de 1 dans la chaine x. Il sera aussi utile de définir le poids de Hamming *relatif* de $x \in \{0,1\}^n$ comme étant $w(x) := wt(x)/n$. Pour $\delta > 0$ et $x \in \{0,1\}^n$, on définit l'ensemble $B^\delta(x) := \{y \in \{0,1\}^n : d(x, y) \leq \delta n\}$ des chaines à distance de Hamming au plus δn de x. Soit $h(p) := -p \log(p) - (1-p) \log(1-p)$ la fonction d'entropie binaire où log est la fonction logarithme en base 2. La relation $\binom{n}{\delta n} \leq 2^{h(\delta)n}$ où $0 < \delta < 1$

implique que l'ensemble $B^{\delta}(x)$ contient au plus $2^{h(\delta)n}$ éléments.

2.2 Théorie des probabilités

Établissons d'abord quelques conventions et éléments de notation. Pour une variable aléatoire X prenant des valeurs dans un ensemble fini Σ, nous écrivons $P_X(x)$ comme raccourci pour $\Pr[X = x]$, pour $x \in \Sigma$. La *valeur espérée* de X est

$$\mathbb{E}[X] := \sum_{x \in \Sigma} P_X(x) \cdot x \ .$$

Celle-ci satisfait *l'inégalité de Markov*

$$\Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a} \tag{2.1}$$

à condition que la variable aléatoire X prenne des valeurs non négatives.

Une fonction $\mathrm{negl} : \mathbb{N} \to \mathbb{R}$ est *négligeable* si pour tout $k \in \mathbb{N}$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $\mathrm{negl}(n) < \frac{1}{n^k}$. On dit qu'un évènement probabiliste $\mathcal{E}_n$, paramétré par un entier n (souvent implicite, mais clair par le contexte) survient avec *probabilité négligeable en* n s'il existe une fonction $\mathrm{negl} : \mathbb{N} \to \mathbb{R}$ telle que $\Pr[\mathcal{E}_n] \leq \mathrm{negl}(n)$.

Théorème 2.2.1 (Inégalité d'Hoeffding)**.** *Soient $X_1, X_2, \ldots, X_n$ des variables aléatoires indépendamment distribuées telles que $0 \leq X_i \leq 1$ pour $i \in [n]$. Soit $\bar{X} := \frac{1}{n}(X_1 + X_2 + \cdots + X_n)$, alors*

$$\Pr[\bar{X} - \mathbb{E}[\bar{X}] \geq t] \leq \exp(-2nt^2) \ .$$

2.3 Information quantique

Cette section introduit les notions d'information quantique qui seront utilisées au courant de cette thèse. Nous suivons une approche similaire à cette de Watrous [Wat11, Wat17] pour introduire ces concepts, commençant par le formalisme en termes d'objets mathématiques, et en décrivant ensuite comment ces objets mathématiques correspondent à des objets physiques et à leurs interactions.

2.3.1 Espaces de Hilbert

Soit $\mathbb{C}^d$ l'espace vectoriel de dimension d sur le corps des complexes. Les éléments de $\mathbb{C}^d$ peuvent être représentés comme des vecteurs colonnes de la forme

$$u = \begin{pmatrix} u(1) \\ \vdots \\ u(d) \end{pmatrix}$$

où $u(1), \ldots, u(d) \in \mathbb{C}$. Le *produit scalaire* $(\cdot, \cdot)$ entre deux vecteurs $u, v \in \mathbb{C}^d$ est une fonction allant de $\mathbb{C}^d \times \mathbb{C}^d$ vers $\mathbb{C}$ qui est définie comme

$$(u, v) := u^* v = \left(\overline{u(1)} \cdots \overline{u(d)}\right) \begin{pmatrix} v(1) \\ \vdots \\ v(d) \end{pmatrix} = \sum_{i=1}^{d} \overline{u(i)} v(i) \tag{2.2}$$

où $u^* = \left(\overline{u(1)} \cdots \overline{u(d)}\right)$ est la transposée conjuguée de u et où $\overline{(a+ib)} = (a-ib)$ est le conjugué complexe. Un espace vectoriel sur le corps des complexes muni d'un produit scalaire $(\cdot, \cdot)$ est appelé un *espace de Hilbert*. Nous utiliserons les lettres scriptées telles $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ pour représenter les espaces de Hilbert et utiliserons la notation de Dirac « $|\cdot\rangle$ » (aussi appelée notation *bra-ket*) pour représenter les vecteurs d'un espace de Hilbert. Dans cette notation, un *ket* $|u\rangle$ représente un vecteur colonne et un *bra* $\langle u|$ représente sa transposée conjuguée (un vecteur ligne), de manière à ce que le produit scalaire entre deux vecteurs $|u\rangle$ et $|v\rangle$ s'écrive simplement $\langle u|v\rangle$. Pour un ensemble de vecteurs $\{|u_1\rangle, \ldots, |u_n\rangle\}$, on définit le *sous-espace engendré* par ces vecteurs comme

$$\text{span}\{|u_1\rangle, \ldots, |u_n\rangle\} := \{\sum_{i=1}^{n} a_i |u_i\rangle \ : \ a_1, \ldots, a_n \in \mathbb{C}\} \ .$$

La *norme euclidienne* d'un vecteur $|u\rangle$ est $\||u\rangle\| := \sqrt{\langle u|u\rangle}$. On dit qu'un vecteur $|u\rangle$ est *normalisé* si $\||u\rangle\| = 1$. La norme euclidienne satisfait plusieurs propriétés, en particulier les trois critères définissant une norme sont

— $\||u\rangle\| \geq 0$,

— $\|\alpha|u\rangle\| = |\alpha| \cdot \||u\rangle\|$ pour tout $\alpha \in \mathbb{C}$ et

— $\||u\rangle + |v\rangle\| \leq \||u\rangle\| + \||v\rangle\|$ (*l'inégalité du triangle*).

Une autre inégalité utile impliquant la norme de vecteurs est *l'inégalité de Cauchy-Schwartz* :

$$|\langle u|v\rangle| \leq \||u\rangle\| \cdot \||v\rangle\| \tag{2.3}$$

Lorsque deux vecteurs $|u\rangle$ et $|v\rangle$ satisfont $\langle u|v\rangle = 0$, on dit alors qu'ils sont *orthogonaux*. Si $\mathcal{X}$ est un espace de Hilbert et $|u_1\rangle, \ldots, |u_d\rangle \in \mathcal{X}$ sont orthogonaux deux à deux, on dit que l'ensemble $\{|u_1\rangle, \ldots, |u_d\rangle\}$ forme une *base* de $\mathcal{X}$ si $\text{span}\{|u_1\rangle, \ldots, |u_d\rangle\} = \mathcal{X}$. On utilise souvent la notation $\{|1\rangle, \ldots, |d\rangle\}$ pour représenter la *base canonique* de $\mathcal{X}$.

2.3.2 Opérateurs linéaires

Soient $\mathcal{X}$ et $\mathcal{Y}$ deux espaces de Hilbert. Définissons $L(\mathcal{X}, \mathcal{Y})$ comme l'ensemble des *opérateurs linéaires* de $\mathcal{X}$ vers $\mathcal{Y}$, c'est-à-dire des fonctions de la forme $A : \mathcal{X} \to \mathcal{Y}$ qui satisfont $A(\alpha|u\rangle + \beta|v\rangle) = \alpha A(|u\rangle) + \beta A(|v\rangle)$ pour tout $|u\rangle, |v\rangle \in \mathcal{X}$ et $\alpha, \beta \in \mathbb{C}$ (nous omettrons les parenthèses et écrirons simplement $A|u\rangle$, par exemple). On utilise la notation $L(\mathcal{X})$ comme raccourci pour $L(\mathcal{X}, \mathcal{X})$ et on écrit $A_{\mathcal{X}\to\mathcal{Y}}$ pour désigner que $A \in L(\mathcal{X}, \mathcal{Y})$ et $A_{\mathcal{X}}$ pour $A \in L(\mathcal{X})$. Il existe une bijection entre les opérateurs linéaires $A \in L(\mathbb{C}^n, \mathbb{C}^m)$ et les matrices de n lignes par m colonnes sur le corps des complexes. Nous ne distinguerons donc pas ces deux objets mathématiques, parlant d'opérateurs linéaires ou de matrices dépendamment de la situation. Notons qu'avec cette analogie avec les matrices, il est facile de voir que l'ensemble $L(\mathcal{X}, \mathcal{Y})$ forme un espace vectoriel avec l'addition matricielle et la multiplication des matrices par un scalaire.

Le *support* d'un opérateur $A \in L(\mathcal{X})$ est l'ensemble

$$\text{supp}(A) := \{|u\rangle \,:\, A|u\rangle \neq 0\} \subseteq \mathcal{X} \ . \tag{2.4}$$

Pour une matrice A, on utilise la notation A^* pour dénoter la *transposée conjuguée* — ou *matrice adjointe* — de A (aussi notée $A^\dagger$ dans d'autres ouvrages). La matrice A^* est l'unique matrice qui satisfait $(A^*|u\rangle, |v\rangle) = (|u\rangle, A|v\rangle)$ où $(\cdot, \cdot)$ est le produit scalaire défini en (2.2). Celle-ci nous permet de définir trois classes importantes d'opérateurs linéaires : pour $A \in L(\mathcal{X})$, on dit que A est

1. *normale* si $A^*A = AA^*$,
2. *hermitienne* si $A^* = A$, et
3. *positive semi-définie* s'il existe $B \in L(\mathcal{X})$ tel que $A = B^*B$.

On peut également définir les matrices positives semi-définies par l'ensemble des matrices $A \in L(\mathcal{X})$ telles que $\langle u|A|u\rangle \geq 0$ pour tout $|u\rangle \in \mathcal{X}$. Lorsque A est positive semi-définie, on écrit $A \geq 0$. Cette notation peut être étendue pour créer un ordre partiel sur l'ensemble des matrices hermitiennes :

$$A \geq B \iff A - B \geq 0 \ . \tag{2.5}$$

Soient $\mathcal{X}$ et $\mathcal{Y}$ deux espaces de Hilbert. On écrit $\mathbb{1}_{\mathcal{X}}$ pour la matrice identité sur $\mathcal{X}$. Si $\mathcal{Z} \subseteq \mathcal{X}$, l'action de $\mathbb{1}_{\mathcal{Z}}$ sur $\mathcal{X}$ est celui de projecteur sur le sous-espace $\mathcal{Z}$ de $\mathcal{X}$ (un *projecteur* est un opérateur P tel que $PP = P$). Une matrice $U \in L(\mathcal{X}, \mathcal{Y})$ est une *isométrie* si $U^*U = \mathbb{1}_{\mathcal{X}}$. Dans le cas spécial d'une isométrie $U \in L(\mathcal{X})$, on dit que U est *unitaire*. On dénote $U(\mathcal{X}, \mathcal{Y})$ l'ensemble des isométries de $\mathcal{X}$ vers $\mathcal{Y}$ et $U(\mathcal{X})$ l'ensemble des unitaires sur $\mathcal{X}$.

Les *vecteurs propres* d'un opérateur A sont les vecteurs $|u\rangle$ tels que $A|u\rangle = \lambda|u\rangle$ pour un $\lambda \in \mathbb{C}$. Dans

ce cas, λ est la *valeur propre* associée à $|u\rangle$. Le théorème suivant est un résultat important sur la structure des opérateurs normaux.

Théorème 2.3.1 (Théorème spectral)**.** *Soit $\mathcal{X}$ un espace de Hilbert, soit $A \in L(\mathcal{X})$ un opérateur normal et soient $\lambda_1, \ldots, \lambda_n$ les valeurs propres de A. Il existe une base $\{|1\rangle, \ldots, |n\rangle\}$ de $\mathcal{X}$ telle que*

$$A = \sum_{i=1}^{n} \lambda_i |i\rangle\langle i| \ . \tag{2.6}$$

Il n'est pas difficile de voir qu'en fait la base $\{|1\rangle, \ldots, |n\rangle\}$ du théorème ci-dessus contient tous les vecteurs propres de A. On appelle (2.6) la *forme spectrale* de A. Celle-ci nous permet de définir l'application de fonctions de la forme $f : \mathbb{C} \to \mathbb{C}$ sur les opérateurs normaux par le biais de

$$f(A) := \sum_{i=1}^{n} f(\lambda_i) |i\rangle\langle i| \tag{2.7}$$

où $\sum_{i=1}^{n} \lambda_i |i\rangle\langle i|$ est la forme spectrale de A.

2.3.3 Produit tensoriel

Le *produit tensoriel* de $\mathcal{X}_1 = \mathbb{C}^{n_1}, \ldots, \mathcal{X}_k = \mathbb{C}^{n_k}$ est

$$\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k = \mathbb{C}^{n_1 \times \cdots \times n_k}$$

Pour $|u_1\rangle \in \mathcal{X}_1, \ldots, |u_k\rangle \in \mathcal{X}_k$, le produit tensoriel $|u_1\rangle \otimes \cdots \otimes |u_k\rangle \in \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k$ de ces vecteurs est défini par

$$|u_1\rangle \otimes \cdots \otimes |u_k\rangle(i_1, \ldots, i_k) := |u_1\rangle(i_1) \cdots |u_k\rangle(i_k) \tag{2.8}$$

où $|v\rangle(i)$ est la i^{e} composante du vecteur $|v\rangle$. Notons que l'espace de Hilbert $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k$ est engendré par les vecteurs de la forme $|u_1\rangle \otimes \cdots \otimes |u_k\rangle$, mais que tous les vecteurs de $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k$ ne sont pas nécessairement de cette forme. Pour $n \in \mathbb{N}$, et un espace de Hilbert $\mathcal{X}$ on écrit $\mathcal{X}^{\otimes n} := \underbrace{\mathcal{X} \otimes \cdots \otimes \mathcal{X}}_{n \text{ fois}}$ cette notation est également utilisée pour les vecteurs ($|u\rangle^{\otimes n} := \underbrace{|u\rangle \otimes \cdots \otimes |u\rangle}_{n \text{ fois}}$) et les opérateurs linéaires (voir (2.11) plus bas).

Pour les opérateurs linéaires $A_1 \in L(\mathcal{X}_1, \mathcal{Y}_1), \ldots, A_k \in L(\mathcal{X}_k, \mathcal{Y}_k)$, on définit le nouvel opérateur

$$A_1 \otimes \cdots \otimes A_k \in L(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k, \mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_k) \tag{2.9}$$

qui est défini par son action sur $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k$, qui est

$$(A_1 \otimes \cdots \otimes A_k)(|u_1\rangle \otimes \cdots \otimes |u_k\rangle) := A_1|u_1\rangle \otimes \cdots \otimes A_k|u_k\rangle \ . \tag{2.10}$$

Puisque les vecteurs de la forme $|u_1\rangle \otimes \cdots \otimes |u_k\rangle$ engendrent l'espace de Hilbert $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k$, l'équation (2.10) définit l'action de $A_1 \otimes \cdots \otimes A_k$ sur tout cet espace par linéarité. Pour un opérateur linéaire $A \in L(\mathcal{X}, \mathcal{Y})$ quelconque, $n \in \mathbb{N}$ et $x \in \{0,1\}^n$, on définit les opérateurs

$$A^{\otimes n} := \underbrace{A \otimes \cdots \otimes A}_{n \text{ fois}} \text{ et } A^{\otimes x} := A^{x_1} \otimes \cdots \otimes A^{x_n} \tag{2.11}$$

où $A^1 := A$ et $A^0 := \mathbb{1}$.

2.3.4 Super-opérateurs

Un *super-opérateur* est une fonction de la forme $\mathcal{E} : L(\mathcal{X}) \to L(\mathcal{Y})$ qui s'applique linéairement sur les éléments de $L(\mathcal{X})$. On écrit $\mathcal{E}_{\mathcal{X}\to\mathcal{Y}}$ pour désigner que $\mathcal{E}$ envoie des éléments de $L(\mathcal{X})$ dans $L(\mathcal{Y})$.

Exemple 2.3.1. La *trace* d'un opérateur linéaire A est le super-opérateur défini par

$$\begin{aligned} \mathrm{tr} : L(\mathcal{X}) &\to \mathbb{C} \\ A &\mapsto \sum_i \langle i|A|i\rangle \end{aligned} \tag{2.12}$$

où $\{|i\rangle\}_i$ forme une base de $\mathcal{X}$.

Le produit tensoriel de plusieurs super-opérateurs peut être défini de manière analogue à celle de plusieurs opérateurs. Soient $\mathcal{E}_1 : L(\mathcal{X}_1) \to L(\mathcal{Y}_1), \ldots, \mathcal{E}_k : L(\mathcal{X}_k) \to L(\mathcal{Y}_k)$, on définit le super-opérateur

$$\mathcal{E}_1 \otimes \cdots \otimes \mathcal{E}_k : L(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k) \to L(\mathcal{Y}_1 \otimes \cdots \otimes \mathcal{Y}_k) \tag{2.13}$$

par son action sur $L(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k)$:

$$(\mathcal{E}_1 \otimes \cdots \otimes \mathcal{E}_k)(A_1 \otimes \cdots \otimes A_k) := \mathcal{E}_1(A_1) \otimes \cdots \otimes \mathcal{E}_k(A_k) \tag{2.14}$$

où $A_i \in L(\mathcal{X}_i)$. Par linéarité, (2.14) définit l'action de $\mathcal{E}_1 \otimes \cdots \otimes \mathcal{E}_k$ sur tout l'espace $L(\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_k)$.

Exemple 2.3.2. La *trace partielle* de $\mathcal{X}$ est le super-opérateur $\mathrm{tr}_{\mathcal{X}} : L(\mathcal{X} \otimes \mathcal{Y}) \to L(\mathcal{Y})$ défini par

$$\mathrm{tr}_{\mathcal{X}}(A \otimes B) := (\mathrm{tr} \otimes \mathrm{id})(A \otimes B) = \mathrm{tr}(A) \otimes B \tag{2.15}$$

où id est le super-opérateur *trivial* agissant sur $L(\mathcal{Y})$ (défini par $\mathrm{id}(A) := A$ pour $A \in L(\mathcal{Y})$) et tr est le super-opérateur de trace défini en (2.12).

Deux classes de super-opérateurs nous intéressent particulièrement (ainsi que leur intersection). Il s'agit d'abord des super-opérateurs $\mathcal{E} : L(\mathcal{X}) \to L(\mathcal{Y})$ *complètement positifs* qui satisfont la propriété que pour tout $\mathcal{Z}$ et pour tout $A \in L(\mathcal{X} \otimes \mathcal{Z})$,

$$A \geq 0 \implies (\mathcal{E} \otimes \mathrm{id})(A) \geq 0 \ . \tag{2.16}$$

Par exemple, la *conjugaison* d'un opérateur $\rho \in L(\mathcal{X})$ par un autre opérateur $A \in L(\mathcal{X}, \mathcal{Y})$ est le super-opérateur complètement positif $\rho \mapsto A\rho A^*$. L'autre classe importante de super-opérateurs sont ceux qui *préservent la trace*, c'est-à-dire les $\mathcal{E} : L(\mathcal{X}) \to L(\mathcal{Y})$ tels que pour tout $A \in L(\mathcal{X})$, $\mathrm{tr}(\mathcal{E}(A)) = \mathrm{tr}(A)$.

Les deux théorèmes suivants offrent des manières intéressantes de caractériser ces deux classes de super-opérateurs.

Théorème 2.3.2 (Caractérisation des opérateurs complètement positifs)**.** *Pour tout super-opérateur $\mathcal{E} : L(\mathcal{X}) \to L(\mathcal{Y})$, les énoncés suivants sont équivalents :*

1. *$\mathcal{E}$ est complètement positif.*
2. *Il existe un ensemble fini d'opérateurs $\{A_i\}_i \subset L(\mathcal{X}, \mathcal{Y})$ tel que*

$$\mathcal{E}(X) = \sum_i A_i X A_i^* \tag{2.17}$$

   pour tout $X \in L(\mathcal{X})$.

3. *Il existe un espace de Hilbert $\mathcal{Z}$ et un opérateur $A \in L(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ tel que*

$$\mathcal{E}(X) = \mathrm{tr}_{\mathcal{Z}}\left(AXA^*\right) \tag{2.18}$$

   pour tout $X \in L(\mathcal{X})$.

Théorème 2.3.3 (Caractérisation des super-opérateurs préservant la trace)**.** *Pour tout super-opérateur $\mathcal{E} : L(\mathcal{X}) \to L(\mathcal{Y})$, les énoncés suivants sont équivalents :*

1. *$\mathcal{E}$ préserve la trace.*
2. *Il existe des ensembles finis d'opérateurs $\{A_i\}_i \subset L(\mathcal{X}, \mathcal{Y})$ et $\{B_i\}_i \subset L(\mathcal{X}, \mathcal{Y})$ tels que*

$$\sum_i B_i^* A_i = \mathbb{1}_{\mathcal{X}} \tag{2.19}$$

   et tels que

$$\mathcal{E}(X) = \sum_i A_i X B_i^* \tag{2.20}$$

   pour tout $X \in L(\mathcal{X})$.

3. *Il existe un espace de Hilbert $\mathcal{Z}$ et deux opérateurs $A, B \in L(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ tels que $B^*A = \mathbb{1}_{\mathcal{X}}$ et*

$$\mathcal{E}(X) = \mathrm{tr}_{\mathcal{Z}}\left(AXB^*\right) \tag{2.21}$$

   pour tout $X \in L(\mathcal{X})$.

Les items 2 et 3 des deux énoncés ci-dessus sont parfois appelés respectivement les représentations de *Kraus* et de *Stinespring*. La preuve de chacun de ces énoncés se trouve dans [Wat11].

2.3.5 Normes sur les opérateurs

Il existe plusieurs normes sur les opérateurs linéaires. Une famille intéressante de normes correspond aux p-normes de la forme

$$\|A\|_p := \left(\mathrm{tr}\left((A^*A)^{p/2}\right)\right)^{1/p} \tag{2.22}$$

lorsque $A \in L(\mathcal{X}, \mathcal{Y})$ pour $p \in \mathbb{N} \cup \{\infty\}$. Pour les différencier de la norme euclidienne $\|\cdot\|$ sur les vecteurs, les normes sur les opérateurs auront toujours en indice la valeur p indiquant à quelle p-norme nous faisons référence.

Chacune des p-normes est invariantes sous les isométries, c'est-à-dire que

$$\|A\|_p = \|UAV^*\|_p \tag{2.23}$$

pour n'importe quelles isométries U, V telles que le produit UAV^* a un sens.

Pour cet ouvrage, deux cas spéciaux de la p-norme nous intéresseront. Il s'agit d'abord du cas où $p = \infty$, que l'on dénote $\|\cdot\|_\infty$ et qui est défini comme

$$\|A\|_\infty := \max\{\|A|u\rangle\| \ : \ |u\rangle \in \mathcal{X}, \||u\rangle\| = 1\} \tag{2.24}$$

où la norme du côté droit de (2.24) est la norme euclidienne. On appelle $\|\cdot\|_\infty$ la *norme spectrale* et elle correspond à la plus grande valeur propre de A. La norme spectrale obéit à l'inégalité suivante :

$$\|ABC\|_p \leq \|A\|_\infty \|B\|_p \|C\|_\infty \tag{2.25}$$

pour $p \in \mathbb{N} \cup \{\infty\}$. L'inégalité suivante impliquant la norme spectrale sera utile.

Lemme 2.3.1 ([Sch07]). *Soient X et Y deux projecteurs, alors $\|X + Y\|_\infty \leq 1 + \|XY\|_\infty$.*

L'autre cas qui nous intéresse est le cas $p = 1$. Dans ce cas on peut simplement écrire $\|A\|_1 = \mathrm{tr}\,|A|$ où $|A| := \sqrt{A^*A}$ est la valeur absolue de A qui peut être définie à l'aide de (2.7) car A^*A est toujours un opérateur positif (donc normal). Une propriété importante de la norme de trace est qu'elle est *monotone* :

$$\|\mathrm{tr}_{\mathcal{Y}}(A)\|_1 \leq \|A\|_1 \tag{2.26}$$

pour tout $A \in L(\mathcal{X} \otimes \mathcal{Y})$. En particulier, $\mathrm{tr}(A) \leq \|A\|_1$.

2.3.6 Registre, états et opérations quantiques

L'élément central de l'information quantique est le *registre quantique*. Un registre est un concept abstrait qui permet de représenter un système physique. Dans cette sous-section, nous allons introduire

l'état d'un registre, les *transformations quantiques* qui modifient l'état d'un registre et les *mesures* qui produisent de l'information classique sur l'état d'un registre.

Tout au long de cet ouvrage, nous utiliserons les majuscules sans empattements du début de l'alphabet [1] (A, B, C, ...) pour représenter des registres quantiques. À tout registre A, on associe un espace de Hilbert qu'on dénote $\mathcal{H}_{\mathsf{A}}$ et qui nous permettra de définir les états et opérations faites sur A en termes des vecteurs, opérateurs et super-opérateurs définis plus tôt dans cette section. Pour deux registres A et B, leur composition $\mathsf{C} = \mathsf{AB}$ est aussi un registre dont l'espace de Hilbert associé est $\mathcal{H}_{\mathsf{C}} = \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$. On dit qu'un registre est *vide* si l'espace de Hilbert associé est de dimension 1. Le plus petit registre non vide est le *qubit*, qui est représenté par un espace de Hilbert à dimension 2.

Pour un registre quantique A, on utilise la notation A^n pour représenter un registre composé de n copies identiques de A et on les numérote par $\mathsf{A}^n = \mathsf{A}_1\mathsf{A}_2 \ldots \mathsf{A}_n$ lorsqu'on doit distinguer les registres individuels.

État d'un registre

L'état d'un registre A est décrit par un opérateur positif semi-défini de trace 1 ρ_{A}, c'est-à-dire un opérateur appartenant à l'ensemble suivant :

$$\mathcal{D}(\mathcal{H}_{\mathsf{A}}) := \{\rho \in L(\mathcal{H}_{\mathsf{A}}) \,:\, \rho \geq 0 \text{ et } \operatorname{tr}(\rho) = 1\} \subset L(\mathcal{H}_{\mathsf{A}}) \ . \tag{2.27}$$

Les éléments de $\mathcal{D}(\mathcal{H}_{\mathsf{A}})$ sont appelés les *opérateurs de densité* sur $\mathcal{H}_{\mathsf{A}}$. On dit que $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}})$ est *pur* si

$$\rho = |\phi\rangle\langle\phi| \tag{2.28}$$

pour un vecteur $|\phi\rangle \in \mathcal{H}_{\mathsf{A}}$. Remarquons que la condition $\operatorname{tr}(\rho) = 1$ implique que $|\phi\rangle$ est un vecteur normalisé. Définissons également l'ensemble

$$\mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{A}}) := \{\rho \in L(\mathcal{H}_{\mathsf{A}}) \,:\, \rho \geq 0 \text{ et } \operatorname{tr}(\rho) \leq 1\} \subset L(\mathcal{H}_{\mathsf{A}}) \ . \tag{2.29}$$

S'il est connu que le registre A est dans un état pur, on décrit alors son état par un vecteur $|\phi\rangle_{\mathsf{A}}$ qui appartient à l'ensemble

$$\mathcal{S}(\mathcal{H}_{\mathsf{A}}) := \{|\phi\rangle \in \mathcal{H}_{\mathsf{A}} \,:\, \||\phi\rangle\| = 1\} \subset \mathcal{H}_{\mathsf{A}} \ . \tag{2.30}$$

On dit de l'état du registre A qu'il est *mixte* s'il n'est pas pur.

1. Les majuscules sans empattements de la fin de l'alphabet (X, Y, Z, ...) représenteront généralement des registres classiques.

Puisque tout opérateur positif semi-défini est normal, le théorème spectral (théorème 2.3.1) implique que tout état mixte peut s'écrire de la forme

$$\rho_{\mathsf{A}} = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|_{\mathsf{A}} \ . \tag{2.31}$$

Puisque $\rho_{\mathsf{A}} \geq 0$ et $\mathrm{tr}(\rho_{\mathsf{A}}) = 1$, on peut en déduire que $\lambda_i \geq 0$ pour tout i et que $\sum_i \lambda_i = 1$. Pour cette raison, les états mixtes sont parfois interprétés comme une *distribution de probabilité* sur les états purs : le registre A est dans l'état $|\phi_i\rangle_{\mathsf{A}}$ avec probabilité λ_i.

Une autre interprétation possible d'un état mixte ρ_{A} est qu'il est l'état d'un sous-registre A appartenant à un plus grand registre AB dont l'état ρ_{AB} est pur. On dit alors que ρ_{AB} *purifie* ρ_{A} et que ρ_{A} est *l'état réduit* de ρ_{AB} obtenu en prenant la trace partielle sur le registre B. Il est facile de voir que tout état mixte A admet une *purification* dans un registre plus grand AB (pour tout registre B tel que $\dim \mathcal{H}_{\mathsf{B}} \geq \dim \mathcal{H}_{\mathsf{A}}$). Soit ρ_{A} dont la décomposition spectrale est donnée par (2.31) et soit $\{|u_i\rangle\}_i$ un ensemble de vecteurs orthogonaux de $\mathcal{H}_{\mathsf{B}}$, alors l'état pur

$$|\Phi\rangle_{\mathsf{AB}} = \sum_i \sqrt{\lambda_i} |\phi_i\rangle_{\mathsf{A}} |u_i\rangle_{\mathsf{B}}$$

purifie ρ_{A} car

$$\mathrm{tr}_{\mathsf{B}} \left(|\Phi\rangle\langle\Phi|_{\mathsf{AB}} \right) = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|_{\mathsf{A}} \ .$$

Remarquons que le choix de l'ensemble $\{|u_i\rangle\}_i$ est arbitraire puisque pour toute isométrie $U \in U(\mathcal{H}_{\mathsf{A}}, \mathcal{H}_{\mathsf{B}})$, $\{U|u_i\rangle\}_i$ forme également un ensemble de vecteurs normalisés orthogonaux. En fait, cette observation se généralise à la propriété suivante des purifications.

Théorème 2.3.4 (Équivalence des purifications)**.** *Soient* $\mathsf{A}, \mathsf{R}_1, \mathsf{R}_2$ *trois registres quantiques et soit* $|\Phi\rangle_{\mathsf{AR}_1}$ *et* $|\Psi\rangle_{\mathsf{AR}_2}$ *deux purifications de* ρ_{A}*, c'est-à-dire tels que*

$$\mathrm{tr}_{\mathsf{R}_1} \left(|\Phi\rangle\langle\Phi|_{\mathsf{AR}_1} \right) = \mathrm{tr}_{\mathsf{R}_2} \left(|\Psi\rangle\langle\Psi|_{\mathsf{AR}_2} \right) = \rho_{\mathsf{A}} \ ,$$

alors il existe une isométrie $U \in U(\mathcal{H}_{\mathsf{R}_1}, \mathcal{H}_{\mathsf{R}_2})$ *telle que* $|\Phi\rangle_{\mathsf{AR}_1} = (\mathbb{1} \otimes U)|\Psi\rangle_{\mathsf{AR}_2}$.

Chaque registre aura une base de préférence, identifiée simplement par $\{|1\rangle_{\mathsf{A}}, \ldots, |n\rangle_{\mathsf{A}}\}$ où $n = \dim \mathcal{H}_{\mathsf{A}}$ qu'on appelle la *base calculatoire*. On dit qu'un registre X est *classique* si son état ρ_{X} est *diagonal* dans la base calculatoire (c'est-à-dire qu'on peut l'écrire sous la forme (2.31) où chaque $|\phi_i\rangle$ appartient à la base calculatoire). On dit que ρ_{XA} est un état *classique-quantique* si X est un registre classique et A est quantique.

Pour les registres à un qubit, deux bases auront une importance particulière pour nos travaux. Il s'agit de la base calculatoire $\{|0\rangle, |1\rangle\}$ et de la *base diagonale* (aussi appelée base de *Hadamard*) composée des

vecteurs $|+\rangle := H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|-\rangle := H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ où

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.32}$$

est la matrice unitaire nommée *transformée de Hadamard*. Cette base s'étend facilement à plusieurs qubits de la manière suivante. À tout $\theta \in \{0,1\}^n$, on associe la base d'un registre de n qubits $\{H^{\otimes\theta}|x\rangle\}_{x\in\{0,1\}^n}$ où $H^{\otimes\theta}$ est défini en (2.11). Par léger abus de langage, on parle de *la base* θ pour désigner l'ensemble $\{H^{\otimes\theta}|x\rangle\}_x$.

Transformations quantiques

Pour faire évoluer l'état d'un registre quantique dans le temps, on lui appliquera certaines transformations. Ces transformations sont modélisées par des super-opérateurs puisqu'elles doivent agir sur l'état d'un registre qui est représenté par un opérateur de densité. Nous utiliserons la notation $\mathcal{E}_{\mathsf{A}\to\mathsf{B}}$ comme raccourcis pour $\mathcal{E}_{\mathcal{H}_\mathsf{A}\to\mathcal{H}_\mathsf{B}}$ (et $\mathcal{E}_\mathsf{A}$ lorsque $\mathsf{A} = \mathsf{B}$) pour désigner un super-opérateur qui prend en entrée un état du registre A et le transforme en un état du registre B. Pour qu'une opération soit physiquement réalisable, elle doit produire en sortie un opérateur de densité, c'est-à-dire un état valide, lorsqu'elle est appliquée sur un opérateur de densité. Ainsi, une transformation prenant en entrée un état du registre A et produisant un état de sortie dans le registre B doit satisfaire les deux conditions suivantes :

— $\mathcal{E}_{\mathsf{A}\to\mathsf{B}}$ est *complètement positive* et

— $\mathcal{E}_{\mathsf{A}\to\mathsf{B}}$ *préserve la trace.*

Ces propriétés sont décrites à la section 2.3.4. Les super-opérateurs satisfaisant ces deux propriétés sont parfois appelés des *CPTP*[2]. Les théorèmes 2.3.2 et 2.3.3 permettent une caractérisation des CPTP en termes d'opérateurs linéaires. Comme pour les super-opérateurs, nous utilisons la notation $V_{\mathsf{A}\to\mathsf{B}}$ comme raccourcis pour $V_{\mathcal{H}_\mathsf{A}\to\mathcal{H}_\mathsf{B}}$ et la notation V_A si $V_\mathsf{A} \in L(\mathcal{H}_\mathsf{A})$.

Une classe spéciale d'opérations quantiques est celle composée des *transformations unitaires* et, plus généralement, des isométries. Ces transformations ont la propriété de transformer un état pur en un autre état pur. Lorsqu'on fait évoluer un registre A dans l'état $|\phi\rangle_\mathsf{A}$ à l'aide d'une isométrie $U_{\mathsf{A}\to\mathsf{B}} \in U(\mathcal{H}_\mathsf{A}, \mathcal{H}_\mathsf{B})$, l'état produit est $U_{\mathsf{A}\to\mathsf{B}}|\phi\rangle \in \mathcal{S}(\mathcal{H}_\mathsf{B})$. Cette opération appliquée sur un état quelconque ρ_A produit l'état

$$U_{\mathsf{A}\to\mathsf{B}}\rho_\mathsf{A}U^*_{\mathsf{A}\to\mathsf{B}} \in \mathcal{D}(\mathcal{H}_\mathsf{B}) \ .$$

Il sera aussi utile de considérer une catégorie de transformations qui ne préservent pas la trace. On appelle ces transformations *CPTN*[3] et elles sont modélisées par les super-opérateurs complètement positifs, mais qui n'augmentent pas la trace. On peut interpréter ces super-opérateurs comme encapsulant à

2. De l'anglais *Completely Positive Trace-Preserving.*
3. De l'anglais *Completely Positive Trace Non-increasing.*

la fois l'action de la transformation et la probabilité que celle-ci survienne. Par exemple, si $\mathcal{E}$ consiste à tirer une pièce et appliquer une certaine opération dépendant du résultat, alors on peut décrire l'action de $\mathcal{E}$ sur un état ρ par

$$\mathcal{E}(\rho) = \mathcal{E}_0(\rho) + \mathcal{E}_1(\rho)$$

où $\mathrm{tr}(\mathcal{E}_0(\rho)) = \mathrm{tr}(\mathcal{E}_1(\rho)) = \frac{1}{2}$. Le super-opérateur $\mathcal{E}$ est un CPTP, alors que $\mathcal{E}_0$ et $\mathcal{E}_1$ sont des CPTNs.

Mesure quantique

Pour extraire de l'information classique sur l'état d'un registre quantique, on doit le soumettre à une *mesure*. Une mesure *destructive*, ou un POVM [4], sur un registre A est décrite par un ensemble d'opérateurs positifs semi-définis $\{E_a\}_{a\in\Sigma} \subset L(\mathcal{H}_\mathsf{A})$ tels que $\sum_{a\in\Sigma} E_a = \mathbb{1}_\mathsf{A}$. L'ensemble Σ représente les résultats possibles de la mesure et les opérateurs E_a correspondants sont appelés les *éléments de POVM*. Lorsqu'une mesure de ce type est effectuée sur le registre quantique A dans l'état ρ_A, deux choses se produisent :

— le résultat $a \in \Sigma$ est obtenu avec probabilité $\mathrm{tr}(E_a\rho_\mathsf{A})$ et

— le registre A est détruit.

Il est possible de représenter une mesure destructrice comme CPTP prenant un registre quantique A et produisant un registre classique X par l'opération

$$\rho_\mathsf{A} \mapsto \sum_{a\in\Sigma} \mathrm{tr}\left(E_a\rho_\mathsf{A}\right) |a\rangle\langle a|_\mathsf{X} \ . \tag{2.33}$$

Il est parfois utile de considérer des mesures qui ne détruisent pas complètement le registre, mais qui produisent un état résiduel. En général, ces mesures perturbent l'état de manière non réversible (c'est-à-dire non unitaire). Soit $\{E_a\}_{a\in\Sigma}$ un POVM, alors puisque chaque $E_a \geq 0$, il existe $M_a \in L(\mathcal{H}_\mathsf{A})$ tel que $M_a^* M_a = E_a$. Considérons alors le CPTP suivant inspiré de (2.33) :

$$\rho_\mathsf{A} \mapsto \sum_{a\in\Sigma} M_a\rho_\mathsf{A}M_a^* \otimes |a\rangle\langle a|_\mathsf{X} \tag{2.34}$$

produisant un état résiduel dans le registre A et le résultat de la mesure dans X. L'état de droite de (2.34) peut être interprété comme étant dans l'état

$$\frac{M_a\rho_\mathsf{A}M_a^*}{\mathrm{tr}\left(M_a\rho_\mathsf{A}M_a^*\right)} \otimes |a\rangle\langle a|_\mathsf{X} \tag{2.35}$$

avec probabilité

$$\mathrm{tr}\left(M_a\rho_\mathsf{A}M_a^*\right) = \mathrm{tr}\left(M_a^*M_a\rho_\mathsf{A}\right) = \mathrm{tr}\left(E_a\rho_\mathsf{A}\right) \ .$$

4. De l'anglais *Positive Operator Valued Measurement*.

Ceci motive la définition de mesure *non destructive* comme une mesure décrite par un ensemble d'opérateurs $\{M_a\}_{a\in\Sigma}$ satisfaisant $\sum_{a\in\Sigma} M_a^* M_a = \mathbb{1}_{\mathsf{A}}$. Cette mesure donne lieu aux mêmes statistiques d'observation que la mesure destructive avec éléments de POVM $E_a = M_a^* M_a$ pour $a \in \Sigma$, mais donne aussi l'état résiduel du registre A (d'où le choix du terme non destructive). Soit X la variable aléatoire représentant le résultat de la mesure, c'est-à-dire prenant la valeur $a \in \Sigma$ avec probabilité $\Pr[X = a] = \mathrm{tr}(M_a^* M_a \rho_{\mathsf{A}})$, alors on définit l'état du registre A *conditionné* sur l'évènement $X = a$ par

$$\rho_{\mathsf{A}}^{X=a} := \frac{M_a \rho_{\mathsf{A}} M_a^*}{\mathrm{tr}\left(M_a \rho_{\mathsf{A}} M_a^*\right)} \tag{2.36}$$

et on écrit simplement ρ_{A}^a lorsque cela ne crée pas d'ambiguïté. Cette définition d'état conditionné s'étend naturellement à tout évènement probabiliste résultant d'une mesure sur un système quantique.

Un type particulier de mesure est la *mesure projective* dont les opérateurs de mesure $\{P_a\}_{a\in\Sigma}$ sont des *projecteurs*, c'est-à-dire des opérateurs qui satisfont la condition $P_a^2 = P_a$. Le théorème suivant dit qu'une mesure destructive peut être simulée par une isométrie suivie d'une mesure projective.

Théorème 2.3.5 (Naimark)**.** *Soit $\{E_a\}_{a\in\Sigma}$ une mesure destructive sur un espace de Hilbert $\mathcal{X}$ et soit $\mathcal{Y}$ tel que $\dim \mathcal{Y} = |\Sigma|$. Alors il existe une isométrie $U \in U(\mathcal{X}, \mathcal{X}\otimes\mathcal{Y})$ telle que*

$$E_a = U^*(\mathbb{1}_{\mathcal{X}} \otimes |a\rangle\langle a|_{\mathcal{Y}})U$$

pour tout $a \in \Sigma$.

2.3.7 Mesures de distance entre états quantiques

Il existe deux outils principalement utilisés pour quantifier le degré de ressemblance de deux états quantiques. Elles ont toutes deux des interprétations opérationnelles importantes et sont intimement liées.

Distance de trace

La *distance de trace* entre deux états quantiques $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ est définie par

$$D(\rho,\sigma) := \frac{1}{2}\left\|\rho - \sigma\right\|_1 \quad . \tag{2.37}$$

Il découle du fait que $\|\cdot\|_1$ est une norme que la distance de trace est une distance au sens mathématique du terme, c'est-à-dire qu'elle satisfait

1. $D(\rho,\sigma) = D(\sigma,\rho)$,
2. $D(\rho,\sigma) \geq 0$ avec $D(\rho,\sigma) = 0 \iff \rho = \sigma$, et

3. $D(\rho,\sigma) \leq D(\rho,\tau) + D(\tau,\sigma)$ pour tout $\tau \in \mathcal{D}(\mathcal{H})$.

Certaines propriétés de la distance de trace sont héritées de la norme de trace. Parmi ces propriétés, on a que la distance de trace est invariante sous les transformations unitaires

$$D(U\rho U^*, U\sigma U^*) = D(\rho,\sigma) \tag{2.38}$$

et qu'elle n'augmente pas sous les transformations quantiques

$$D(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \leq D(\rho,\sigma) \tag{2.39}$$

où $\mathcal{E}$ est un CPTP.

En particulier, la relation (2.39) nous dit que toute mesure donnant lieu à un résultat classique X_ρ lorsque faite sur ρ et X_σ sur σ satisfait $D(P_{X_\rho}, P_{X_\sigma}) \leq D(\rho,\sigma)$ où

$$D(P_{X_\rho}, P_{X_\sigma}) := \frac{1}{2}\sum_x |P_{X_\rho}(x) - P_{X_\sigma}(x)|$$

est la distance de trace entre deux distributions de probabilité. Ceci implique l'interprétation suivante de la norme de trace : si $D(\rho,\sigma) \leq \epsilon$, alors ρ *se comporte de manière identique à* σ, sauf avec probabilité ϵ. Cette interprétation est formalisée par la proposition suivante [Ren05].

Proposition 2.3.1. *Soient X et X' deux variables aléatoires avec distributions de probabilité respectives P_X et $P_{X'}$. Alors il existe une distribution conjointe $P_{XX'}$ telle que les distributions marginales de $P_{XX'}$ correspondent à P_X et $P_{X'}$ et telle que*

$$\Pr[X \neq X'] \leq D(P_X, P_{X'})$$

Le lemme suivant dit essentiellement que si un résultat particulier d'une mesure effectuée sur ρ est très probable, alors cette mesure ne perturbe pas trop l'état ρ.

Lemme 2.3.2 (*Gentle Measurement Lemma* [Win99, ON02])**.** *Soit $\rho \in \mathcal{D}(\mathcal{H})$ et soit $0 \leq E \leq \mathbb{1}$. Alors*

$$D(\rho, \sqrt{E}\rho\sqrt{E}) \leq \sqrt{1 - \operatorname{tr}(E\rho)}$$

Fidélité

La fidélité de deux états quantiques $\rho,\sigma \in \mathcal{D}(\mathcal{H})$ est définie par

$$F(\rho,\sigma) := \operatorname{tr}\left(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right) \quad . \tag{2.40}$$

La fidélité représente une mesure de *proximité* de ρ et σ car $F(\rho,\sigma) = 1 \iff \rho = \sigma$. Il est facile de vérifier que la fidélité est aussi invariante sous les opérations unitaires et qu'elle est monotone sous l'application de transformations quantiques :

$$F(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \geq F(\rho,\sigma) \tag{2.41}$$

où $\mathcal{E}$ est un CPTP. La fidélité satisfait également $F(\rho,\sigma) = F(\sigma,\rho)$.

Une propriété très utile de la fidélité est le théorème d'Uhlmann qui dit que la fidélité entre deux états mixtes correspond au plus grand produit scalaire entre deux purifications de ces états.

Théorème 2.3.6 (Uhlmann)**.** *Soient $\rho,\sigma \in \mathcal{D}(\mathcal{H})$ et soit $|\phi\rangle$ une purification de ρ. Alors*

$$F(\rho,\sigma) = \max_{|\psi\rangle} |\langle\psi|\phi\rangle|$$

où le maximum est sur toutes les purifications $|\psi\rangle$ de σ.

Relation entre la fidélité et la distance de trace

La fidélité et la distance de trace peuvent être reliées par l'équation suivante :

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2} \ . \tag{2.42}$$

L'expression (2.42) porte parfois le nom *d'inégalités de Fuchs-van de Graaf*. On peut aussi inverser la fidélité et la distance de trace dans ces inégalités :

$$1 - D(\rho,\sigma) \leq F(\rho,\sigma) \leq \sqrt{1 - D(\rho,\sigma)^2} \ . \tag{2.43}$$

La propriété suivante de la distance de trace peut être facilement prouvée à l'aide des propriétés de la *distance purifiée* [Tom12], une mesure de distance qui a de belles propriétés, mais qui ne nous sera pas nécessaire pour cet ouvrage.

Proposition 2.3.2. *Soient $\sigma,\rho \in \mathcal{D}_{\leq}(\mathcal{H})$, alors pour toute purification $|\sigma\rangle$ de σ il existe une purification $|\rho\rangle$ de ρ telle que*

$$\frac{1}{2} \left\| |\sigma\rangle\langle\sigma| - |\rho\rangle\langle\rho| \right\|_1 \leq \|\sigma - \rho\|_1^{\frac{1}{2}} \ . \tag{2.44}$$

2.4 Évaluation sûre à deux participants

Une *primitive cryptographique* est une tâche cryptographique entre deux [5] participants qui, par convention, sont nommés *Alice* et *Bob*. Cette tâche spécifie un comportement d'entrée/sortie que les participants tenteront de reproduire par un protocole. Par exemple, la primitive ÉCH correspond à l'échange honnête (ou instantané) de message. Pour une certaine tâche, la *fonctionnalité idéale* associée à cette tâche est une machine $\mathcal{F}$ qui reproduit le comportement d'entrée/sortie spécifiée par la primitive. Pour l'exemple

5. Il existe un riche champ de recherche sur les tâches cryptographiques à plus de deux participants, mais dans cette thèse, nous nous limiterons aux tâches entre deux parties.

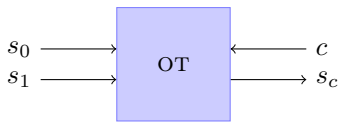
ci-dessus, $\mathcal{F}_{\text{ÉCH}}$ prend en entrée a et b et donne en sortie b et a. Cette association est bijective puisque pour toute primitive on peut définir une fonctionnalité qui l'implémente et à chaque fonctionnalité on peut associer une primitive qui correspond à la tâche que réalise cette fonctionnalité. Ainsi, nous utiliserons les termes primitives et fonctionnalités de manière interchangeable.

La façon la plus simple de définir une primitive cryptographique est par le comportement d'entrée/sortie de sa fonctionnalité idéale. Voici quelques exemples de primitives que nous rencontrerons dans cette thèse.

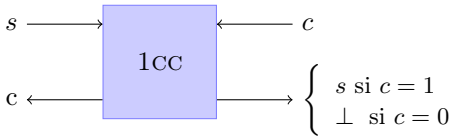
Exemple 2.4.1.

- transfert équivoque (OT) : Alice (l'envoyeuse) envoie deux bits (s_0, s_1) à $\mathcal{F}_{\text{OT}}$ et Bob (le receveur) envoie un bit de sélection $c \in \{0,1\}$. Bob reçoit s_c de $\mathcal{F}_{\text{OT}}$ et Alice ne reçoit aucune sortie.
- mise en gage (BC) : Alice (l'envoyeuse) envoie un bit b à $\mathcal{F}_{\text{BC}}$ et Bob reçoit un message « `mis en gage` ». Plus tard, Alice peut envoyer le message « `ouvrir` » à $\mathcal{F}_{\text{BC}}$ auquel cas $\mathcal{F}_{\text{BC}}$ envoie b à Bob.
- transfert sélectif à m bits (mCC) : Alice envoie un message $s \in \{0,1\}^m$ à $\mathcal{F}_{m\text{CC}}$ et Bob envoie un bit c. Bob reçoit s si $c = 1$ et $\perp$ sinon, et Alice reçoit c.
- *OU exclusif* (XOR) : Alice et Bob entrent les bits x et y, respectivement, dans $\mathcal{F}_{\text{XOR}}$, ils reçoivent chacun $x \oplus y$ (équivalent à la fonctionnalité $\mathcal{F}_{\text{ÉCH}}$ décrite plus haut).
- Le *tirage d'une pièce* (CT) : Alice et Bob n'ont pas d'entrée, il reçoivent tous les deux le même bit x uniformément distribué de la fonctionnalité $\mathcal{F}_{\text{CT}}$.

Les fonctionnalités idéales $\mathcal{F}$ sont souvent représentées comme des *boîtes noires* (voir figures 2.1 et 2.2) dont le fonctionnement interne est inconnu, mais qui ont un comportement d'entrée/sortie décrit par $\mathcal{F}$.



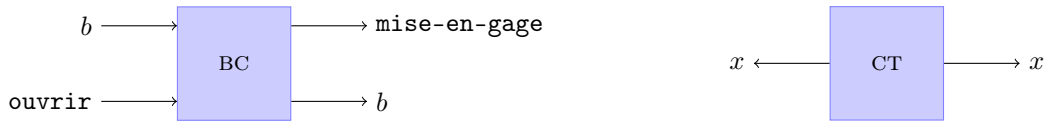
(a) transfert équivoque



(b) transfert sélectif

FIGURE 2.1 – Les fonctionnalités transfert équivoque et transfert sélectif

Pour implémenter une primitive cryptographique, Alice et Bob auront recours à un protocole Π qui tente d'implémenter la fonctionnalité idéale associée $\mathcal{F}$. De manière intuitive, on dit d'un protocole qu'il est *sécuritaire* — ou *sûr* — s'il reproduit fidèlement le comportement de la fonctionnalité $\mathcal{F}$. Il existe plus d'une manière de définir la sécurité d'un protocole Π. Dans tous les cas, il s'agit de montrer qu'un *adversaire* qui *corrompt* un participant ne gagne pas à interagir avec Π plutôt qu'avec $\mathcal{F}$. Intuitivement, cela implique que le protocole Π est *autant sûr* que la fonctionnalité idéale $\mathcal{F}$ qui, elle, est sûre par définition. Les preuves de sécurité pour les protocoles implémentant des primitives à deux participants



(a) mise en gage (b) tirage d'une pièce

FIGURE 2.2 – Les fonctionnalités mise en gage et tirage d'une pièce. Pour la primitive $\mathcal{F}_{\text{BC}}$, les messages sont séquentiels du haut vers le bas ; Alice envoie d'abord un bit b dans la primitive qui envoie le message `mise-en-gage` à Bob, ensuite Alice peut envoyer un message `ouvrir` à la primitive qui enverra alors le bit b à Bob.

auront deux volets : il faut montrer la sécurité pour chacun des participants corrompus (on dit aussi que le participant est *malhonnête*).

Les définitions de sécurité présentées dans cette section font appel à la notion de *simulation*. Il s'agit des notions de sécurité les plus strictes et qui offrent les meilleures garanties de composabilité des protocoles. Pour montrer la sécurité d'un protocole Π, on associe à chaque adversaire interagissant avec Π un *simulateur* qui doit imiter, d'un point de vue externe, les actions de l'adversaire, mais qui lui interagit avec $\mathcal{F}$. Le terme « simulateur » vient du fait qu'il peut simuler de manière interne l'attaque de l'adversaire sur le protocole Π. Cette notion de simulation sert à formaliser l'énoncé « tout ce que l'adversaire peut faire contre Π, le simulateur peut le faire contre $\mathcal{F}$ ». Chacune des définitions est présentée de manière informelle, car introduire les notions nécessaires à les énoncer formellement alourdirait inutilement cet ouvrage. Ces définitions donnent toutefois une bonne idée de ce qui est requis pour montrer la sécurité dans chacun de ces modèles et nous donnerons des références où chacune des définitions est énoncée formellement.

Sauf lorsque spécifié autrement, les protocoles, définitions de sécurité et notions de réduction et de complétude qui en découlent sont supposés quantiques.

2.4.1 La sécurité autonome

Le modèle de *sécurité autonome* [FS09, WW08] est défini comme suit. Un protocole Π est sûr dans ce modèle si pour tout adversaire contre le protocole, il existe un simulateur qui interagit avec $\mathcal{F}$ capable de produire un état final $\rho_{\text{idéal}}$ arbitrairement près de l'état final $\rho_{\text{réel}}$ de l'adversaire interagissant avec Π.

Définition 2.4.1 (Sécurité autonome quantique — informel)**.** Un protocole Π *implémente* une fonctionnalité idéale $\mathcal{F}$ de manière sûre dans le modèle à sécurité autonome si pour tout participant [6] $p \subset \{\text{Alice}, \text{Bob}\}$

6. Nous ignorons le cas $p = \{Alice, Bob\}$ où les deux participants sont corrompus.

et pour tout adversaire Adv qui corrompt le participant p, il existe un simulateur Sim tel que l'état final *réel* de l'exécution de Π avec Adv est indistinguable [7] de l'état final *idéal* de l'exécution de $\mathcal{F}$ avec Sim.

Le cas $p = \emptyset$ dans la définition ci-dessus correspond au cas où les deux participants sont honnêtes. Dans ce cas, la définition implique la *correction* [8] du protocole Π, c'est-à-dire que Π implémente bien $\mathcal{F}$ lorsque les participants sont honnêtes. Nous ne considérerons jamais le cas où les deux participants sont corrompus.

2.4.2 La sécurité universellement composable

Le modèle de sécurité *universellement composable* est défini de manière similaire au modèle autonome, mais impose des conditions supplémentaires sur la qualité de la simulation de l'adversaire. Il ne suffit plus que le simulateur produise un état final indistinguable de celui de l'adversaire pour toute entrée au protocole, il doit aussi être indistinguable de l'adversaire du point de vue d'un *environnement* — une entité externe qui peut interagir avec l'adversaire par le biais d'une interface arbitraire. En particulier, l'environnement fournit l'entrée du protocole aux participants, peut spécifier des instructions à l'adversaire, reçoit les sorties des participants, etc. Le simulateur doit donc offrir la même interface à l'environnement et agir de manière indistinguable de l'adversaire réel (du point de vue de l'environnement) tout en interagissant avec la fonctionnalité idéale $\mathcal{F}$ au lieu du protocole Π.

Le modèle universellement composable dans le monde classique fut introduit par Canetti [Can01]. Nous utiliserons l'extension dans le monde quantique proposée par Unruh [Unr10].

Définition 2.4.2 (Sécurité UC quantique — informel)**.** Un protocole Π *implémente* une fonctionnalité idéale $\mathcal{F}$ de manière sûre dans le modèle UC si pour tout participant $p \subset \{\text{Alice}, \text{Bob}\}$ et pour tout adversaire Adv qui corrompt le participant p, il existe un simulateur Sim tel que pour tout environnement Env, le modèle *réel* où Adv interagit avec Π et Env est indistinguable [9] du modèle *idéal* où Sim interagit avec $\mathcal{F}$ et Env. De plus, le temps d'exécution de Sim doit être polynomial dans le temps d'exécution de Adv.

Les modèles réel et idéal de la définition ci-dessus sont présentés sous forme de réseaux dans la figure 2.3 pour le cas où Alice est corrompue. Le cas $p = \emptyset$ correspond à la situation où les deux participants sont honnêtes. Comme pour la définition 2.4.1, la définition 2.4.2 implique la correction du protocole Π dans

7. Deux états sont indistinguables si leur distance de trace est négligeable.
8. Le terme « correction » est employé ici avec le sens « caractère de ce qui est correct, conforme aux règles ».
9. Les deux modèles doivent être indistinguables au sens *statistique* du terme. C'est-à-dire qu'aucun environnement (même avec une puissance de calcul non bornée) ne peut distinguer les deux modèles avec probabilité meilleure que négligeable.

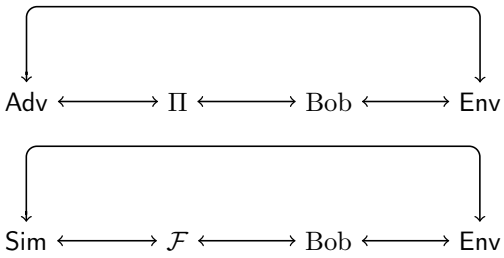


FIGURE 2.3 – Le modèle réel (haut) et le modèle idéal (bas) pour le protocole Π et la fonctionnalité idéale $\mathcal{F}$, respectivement, avec Alice malhonnête. Dans le modèle idéal, le participant honnête ne fait que faire suivre les messages allant de Env à $\mathcal{F}$, et vice versa. Le protocole Π implémente $\mathcal{F}$ dans le modèle UC (contre Alice malhonnête) si pour tout Adv, il existe Sim tel que pour tout Env, les deux modèles sont indistinguables.

ce cas. On dit d'un protocole Π qu'il implémente $\mathcal{F}$ de manière UC-sûre s'il satisfait la définition 2.4.2 et on dit simplement qu'il est UC-sûr si $\mathcal{F}$ est évident par le contexte.

2.4.3 Composabilité et modèles hybrides

Il est possible de concevoir des protocoles cryptographiques Π qui font appel à des fonctionnalités idéales $\mathcal{F}$ en tant que *sous-routines*. On dit alors que Π est dans le *modèle $\mathcal{F}$-hybride* et on écrit $\Pi^{\mathcal{F}}$. En pratique, on voudra remplacer les occurrences de $\mathcal{F}$ dans $\Pi^{\mathcal{F}}$ par un protocole Π' qui implémente de manière sûre la fonctionnalité $\mathcal{F}$. Le protocole résultant restera sûr selon la manière dont les primitives $\mathcal{F}$ sont utilisées à l'intérieur de $\Pi^{\mathcal{F}}$ et la définition de sécurité que satisfait Π'.

La définition 2.4.1 garantit la *composabilité séquentielle* des protocoles, c'est-à-dire que si $\Pi_1, \ldots, \Pi_n$ sont des protocoles pour $\mathcal{F}_1, \ldots, \mathcal{F}_n$, respectivement, qui sont sûrs selon la définition 2.4.1, alors tout protocole Π qui fait des appels *séquentiels* à $\mathcal{F}_1, \ldots, \mathcal{F}_n$ peut remplacer ces fonctionnalités idéales par les protocoles respectifs $\Pi_1, \ldots, \Pi_n$ tout en étant aussi sûr que lorsqu'il utilise les primitives, pourvu que l'exécution de Π_i soit terminée avant celle de Π_{i+1}. Cette définition n'offre par contre aucune garantie de sécurité si les appels à $\mathcal{F}_1, \ldots, \mathcal{F}_n$ sont faits en parallèle.

La définition 2.4.2 peut être considérée la notion de sécurité la plus forte pour les protocoles quantiques. Comme le nom l'indique, les protocoles qui sont sûrs selon cette définition sont *universellement composables*, c'est-à-dire que pour tout protocole $\Pi^{\mathcal{F}}$ dans le modèle $\mathcal{F}$-hybride, on peut remplacer $\mathcal{F}$ par un protocole Π' qui implémente $\mathcal{F}$ de manière sûre dans le modèle UC (définition 2.4.2) peu importe de quelle manière les appels à $\mathcal{F}$ sont effectués. Cela tient également lorsque plusieurs fonctionnalités $\mathcal{F}_1, \ldots, \mathcal{F}_n$ sont implémentées par $\Pi_1, \ldots, \Pi_n$ de manière UC-sûre.

2.4.4 Réductions et complétude

Le modèle $\mathcal{F}$-hybride nous permet de définir la notion de *réduction* de primitives cryptographiques. Soit $\mathcal{F}$ et $\mathcal{F}'$ deux fonctionnalités idéales, on dit que $\mathcal{F}'$ se réduit à $\mathcal{F}$ (et on écrit $\mathcal{F}' \sqsubseteq \mathcal{F}$) dans le modèle UC s'il existe un protocole $\Pi^{\mathcal{F}}$ dans le modèle $\mathcal{F}$-hybride qui implémente $\mathcal{F}'$ de manière UC-sûre. Il existe plusieurs types de réductions, en fonction de la définition de sécurité qu'on emploie, mais dans cette thèse, nous utiliserons uniquement la réduction dans le modèle UC, c'est-à-dire telle que définie ci-dessus.

Les réductions nous permettent de classer les fonctionnalités selon leur *puissance cryptographique*. Une primitive $\mathcal{F}$ est *au moins aussi puissante que* $\mathcal{F}'$ si $\mathcal{F}' \sqsubseteq \mathcal{F}$. La relation « $\sqsubseteq$ » est transitive et induit une relation d'équivalence sur l'ensemble des fonctionnalités idéales où $\mathcal{F} \equiv \mathcal{F}'$ si $\mathcal{F}' \sqsubseteq \mathcal{F}$ et $\mathcal{F} \sqsubseteq \mathcal{F}'$. Parmi les classes d'équivalences importantes, on trouve les primitives *triviales* ou *réalisables*, c'est-à-dire les fonctionnalités $\mathcal{F}$ telles qu'il existe un protocole Π qui implémente $\mathcal{F}$ de manière UC-sûre sans hypothèse. À l'autre extrême, les primitives *complètes* ou *universelles* sont l'ensemble des primitives $\mathcal{F}$ telles que pour toute primitive $\mathcal{F}'$, $\mathcal{F}' \sqsubseteq \mathcal{F}$. Autrement dit, si $\mathcal{F}$ est complète, alors pour n'importe quelle primitive $\mathcal{F}'$, il existe un protocole $\Pi^{\mathcal{F}}$ dans le modèle $\mathcal{F}$-hybride qui implémente $\mathcal{F}'$ de manière UC-sûre. On dit qu'une primitive est complète (ou triviale) si la fonctionnalité correspondante l'est.

Il est utile de noter que toute réduction dans le modèle UC classique implique la même réduction dans le modèle UC quantique [Unr10]. En particulier, toute primitive qui est complète classiquement l'est aussi quantiquement. L'inverse n'est pas vrai ; il existe des primitives complètes quantiquement qui ne le sont pas classiquement.

Le théorème suivant compile deux résultats importants pour le calcul sûr biparti.

Théorème 2.4.1.

- [Kil88, IPS08] *La primitive* OT *est complète dans le modèle UC classique (donc aussi quantique).*
- [Unr10, DFL$^+$09, BBCS91, BF10, PR08] *La primitive* BC *est complète dans le modèle UC quantique.*

La primitive OT est parfois présentée comme l'exemple canonique d'une primitive complète. On cherchera ainsi à réduire $\mathcal{F}_{\text{OT}}$ ou $\mathcal{F}_{\text{BC}}$ à $\mathcal{F}$ pour montrer que la fonctionnalité $\mathcal{F}$ est complète dans le modèle UC classique ou quantique, respectivement.

La caractérisation suivante des primitives cryptographiques dans le modèle UC quantique provient de [FKS$^+$13]. Leur caractérisation s'applique à toutes les fonctionnalités $\mathcal{F}$, sauf celles qui permettent d'implémenter $\mathcal{F}_{1\text{CC}}$, mais pas $\mathcal{F}_{2\text{CC}}$. La complétude de $\mathcal{F}_{1\text{CC}}$ fut prouvée dans [DFLS16a], complétant ainsi le portrait des primitives dressé par [FKS$^+$13].

Théorème 2.4.2 (Classification des primitives dans le modèle UC quantique)**.** *Une fonctionnalité $\mathcal{F}$, dans le modèle UC quantique, est*

1. *soit complète,*
2. *soit triviale, ou*
3. *soit équivalente à $\mathcal{F}_{\text{XOR}}$.*

Le théorème suivant montre qu'il est impossible d'obtenir une telle classification dans le monde classique (sans hypothèse calculatoire).

Théorème 2.4.3 ([MPR09, KMQ11a, FKS+13])**.** *Il existe une* hiérarchie stricte *de primitives de type transfert sélectif dans le modèle UC classique :*

$$\mathcal{F}_{1\text{CC}} \not\sqsubseteq \mathcal{F}_{2\text{CC}} \not\sqsubseteq \cdots \not\sqsubseteq \mathcal{F}_{m\text{CC}} \not\sqsubseteq \cdots$$

où chaque membre de la hiérarchie est défini par la taille de l'entrée $m \in \mathbb{N}$.

2.5 Théorie de l'information (quantique)

La théorie de l'information est un riche champ d'études introduit par Shannon en 1949 [Sha49]. Elle trouve de nombreuses applications pour la transmission de messages par un canal bruité, pour la correction d'erreur et pour la cryptographie. Une quantité importante en théorie de l'information est *l'entropie*. Dans le cas classique, celle-ci quantifie l'incertitude en moyenne qu'on a sur la valeur que peut prendre la réalisation d'une variable aléatoire. Il existe différentes notions d'entropie pour les variables aléatoires classiques avec les généralisations correspondantes pour la théorie de l'information quantique. Nous n'utiliserons dans ce document que deux mesures d'information, soit la *min-entropie* et la *max-entropie*[10] (définies plus bas) qui correspondent respectivement au cas $\alpha = \infty$ et $\alpha = 0$ de l'entropie de Rényi H_α [Rén61]. L'avantage de ces deux cas particuliers dans un contexte cryptographique est qu'elles ont des interprétations opérationnelles en termes de *pire cas* au lieu de décrire le comportement *en moyenne* d'une variable aléatoire.

Définition 2.5.1 (min-entropie)**.** Soit $\rho_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ l'état conjoint de deux registres quantiques A et B. La min-entropie de A conditionnée sur le registre B pour l'état ρ_{AB} est

$$\text{H}_\infty(\mathsf{A}|\mathsf{B})_\rho = \max_{\sigma_{\mathsf{B}}} \sup\{\lambda \in \mathbb{R} \,:\, 2^{-\lambda} \cdot \mathbb{1}_{\mathsf{A}} \otimes \sigma_{\mathsf{B}} \geq \rho_{\mathsf{AB}}\}$$

où le maximum est sur tous les états $\sigma_{\mathsf{B}} \in \mathcal{D}(\mathcal{H}_{\mathsf{B}})$.

10. Il existe deux définitions de ce terme dans la littérature, soit le cas $\alpha = 0$ et le cas $\alpha = \frac{1}{2}$ de l'entropie de Rényi H_α. Comme nous n'utiliserons que le premier cas dans cette thèse, nous utilisons le terme max-entropie pour désigner H_0.

Quand l'état ρ_{AB} est clair selon le contexte, nous écrivons parfois $\mathrm{H}_\infty(\mathsf{A}|\mathsf{B})$ au lieu de $\mathrm{H}_\infty(\mathsf{A}|\mathsf{B})_\rho$. Quand le registre B est *vide* on parle alors de la min-entropie de ρ_{A}. Cette quantité est égale à

$$\mathrm{H}_\infty(\mathsf{A})_\rho = -\log \lambda_{\max}(\rho_{\mathsf{A}}) \tag{2.45}$$

où $\lambda_{\max}(\rho_{\mathsf{A}})$ désigne la plus grande valeur propre de ρ_{A}. Par l'expression (2.45), on obtient directement que la min-entropie $\mathrm{H}_\infty(X)$ d'une variable aléatoire X est donnée par $\mathrm{H}_\infty(\rho_{\mathsf{X}})$ où

$$\rho_{\mathsf{X}} = \sum_x P_X(x)|x\rangle\langle x|_{\mathsf{X}} \ .$$

Si ρ_{XA} est un état classique-quantique, la min-entropie de X conditionnée sur le registre A a l'interprétation opérationnelle suivante.

$$\mathrm{H}_\infty(\mathsf{X}|\mathsf{A})_\rho = -\log P_{\mathrm{dev}}(\mathsf{X}|\mathsf{A})_\rho \tag{2.46}$$

où $P_{\mathrm{dev}}(\mathsf{X}|\mathsf{A})_\rho$ correspond à la probabilité maximale de deviner la valeur classique que contient le registre X à partir du registre A. Formellement,

$$P_{\mathrm{dev}}(\mathsf{X}|\mathsf{A})_\rho = \max_{\{M_x\}} \sum_x \mathrm{tr}\left((|x\rangle\langle x|_{\mathsf{X}} \otimes M_x)\rho_{\mathsf{XA}}\right) \tag{2.47}$$

où le maximum est sur tous les POVM $\{M_x\}_x$ sur le registre A.

Définition 2.5.2 (max-entropie)**.** Soit $\rho_{\mathsf{A}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}})$, la *max-entropie* de ρ_{A} est

$$\mathrm{H}_0(\mathsf{A})_\rho = \log \ \mathrm{rang}\, \rho_{\mathsf{A}} \ .$$

La proposition suivante établit une relation utile entre la min- et la max-entropie.

Proposition 2.5.1 (règle de chaine [Ren05])**.** *Soient* A*,* B *et* C *des registres quantiques, alors*

$$\mathrm{H}_\infty(\mathsf{A}|\mathsf{BC}) \geq \mathrm{H}_\infty(\mathsf{A}|\mathsf{B}) - \mathrm{H}_0(\mathsf{C}) \ .$$

2.6 Amplification de l'incertitude

Supposons qu'un participant dispose d'une clé secrète sur laquelle un adversaire connaît une certaine quantité d'information. On appelle cette information *l'information auxiliaire*. Le participant peut *amplifier* l'incertitude de l'adversaire sur cette clé en appliquant une certaine opération à sa clé et obtenir une nouvelle clé, plus courte, mais (presque) complètement aléatoire du point de vue de l'adversaire. Cette section présente ce résultat connu sous le nom *d'amplification de l'incertitude*. L'amplification de l'incertitude existe depuis longtemps dans le cas d'information auxiliaire classique [BBR88, BBCM95]. Dans le

cas d'information auxiliaire quantique, celui qui nous intéresse, Renner [Ren05] a montré que cette tâche est également possible.

L'outil de base pour l'amplification de l'incertitude est la *fonction de hachage*.

Définition 2.6.1. Soit $\mathcal{F}$ une famille de fonctions de hachage de la forme $f : X \to Z$ et soit P_F une distribution de probabilité sur $\mathcal{F}$. La paire $(\mathcal{F}, P_F)$ est dite 2-*universelle* si pour tout $x \neq x' \in X$,

$$\Pr[F(x) = F(x')] \leq \frac{1}{|Z|}$$

où F est choisie aléatoirement selon la distribution P_F.

Le lemme suivant garantit l'existence de familles de fonctions de hachage respectant la définition précédente.

Lemme 2.6.1 ([Ren05, CW79, WC81])**.** *Soit $0 \leq \ell \leq n$. Il existe une famille 2-universelle de fonctions de hachage de la forme $f : \{0,1\}^n \to \{0,1\}^\ell$.*

L'énoncé formel de l'amplification de l'incertitude est le suivant.

Théorème 2.6.1 (Amplification de l'incertitude [RK05, Ren05])**.** *Soit $\rho_{\mathsf{XA}} = \sum_x P_X(x)|x\rangle\langle x|_{\mathsf{X}} \otimes \rho^x_{\mathsf{A}}$ un état classique-quantique avec base orthonormale $\{|x\rangle\}_{x\{0,1\}^n}$ pour $\mathcal{H}_{\mathsf{X}}$ et soit $\mathcal{F}$ une famille de fonctions de hachage 2-universelle de $\{0,1\}^n$ dans $\{0,1\}^\ell$. Alors*

$$D(\rho_{\mathsf{ZFA}}, \frac{\mathbb{1}_{\mathsf{Z}}}{2^\ell} \otimes \rho_{\mathsf{FA}}) \leq 2^{-\frac{1}{2}(\mathrm{H}_\infty(\rho_{\mathsf{XA}}|\mathsf{A})-\ell)}$$

où $\rho_{\mathsf{ZFA}} = \sum_f \sum_x P_F(f)P_X(x)|f(x)\rangle\langle f(x)|_{\mathsf{Z}} \otimes |f\rangle\langle f| \otimes \rho^x_{\mathsf{A}}$ et où $D(\cdot,\cdot)$ est la distance de trace définie dans la section 2.3.7.

Lorsqu'un participant détient une clé sur laquelle l'adversaire détient de l'information auxiliaire dans un registre quantique A, appliquer une fonction de hachage aléatoire sur le registre classique X contenant cette clé donne un résultat indistinguable d'une variable aléatoire uniforme sur ℓ bits, même lorsqu'on conditionne sur le registre A et la fonction de hachage appliquée. Par la discussion entourant la distance de trace à la section 2.3.7, on peut conclure que la clé résultant de l'application de la fonction de hachage *est* uniformément distribuée, sauf avec probabilité négligeable.

2.7 Codes correcteurs linéaires

Un *code correcteur linéaire*, dans son expression la plus simple, est un ensemble de *mots de codes*. Les codes correcteurs [11] sont utilisés en pratique pour encoder l'information de manière résiliente aux erreurs, mais nous les utiliserons pour leurs autres propriétés décrites dans cette section. Nous nous restreindrons aux codes correcteurs *booléens*. Une manière commode de décrire un tel code C est de le considérer comme un sous-espace de $\mathbb{F}_2^n$, où $\mathbb{F}_2$ est le corps fini à deux éléments. On dit que C est un $[n, k]$-code si $\dim C = k$. Il existe deux manières équivalentes de définir un $[n, k]$-code :

1. par une *matrice génératrice* $G \in L(\mathbb{F}_2^k, \mathbb{F}_2^n)$, auquel cas les éléments de C sont les combinaisons linéaires des vecteurs lignes de G, ou
2. par une *matrice de parité* $H \in L(\mathbb{F}_2^n, \mathbb{F}_2^{n-k})$, auquel cas les éléments de C sont les vecteurs $x \in \mathbb{F}_2^n$ tels que $Hx = 0^{n-k}$.

Si H est la matrice de parité de C et $x \in \mathbb{F}_2^n$, on appelle la chaine $s = Hx \in \mathbb{F}_2^{n-k}$ le *syndrome* de x pour le code C.

On dit qu'un code C est un $[n, k, d]$-code correcteur si $d(u, v) \geq d$ pour tout $u, v \in C$. L'énoncé suivant donne une propriété importante des $[n, k, d]$-codes.

Propriété 2.7.1. *Si C est un $[n, k, d]$-code correcteur avec matrice de parité $H \in L(\mathbb{F}_2^n, \mathbb{F}_2^{n-k})$, alors pour tous $x, x' \in \mathbb{F}_2^n$ tels que $Hx = Hx' = s$ satisfont $d(x, x') \geq d$*

Le résultat suivant (et son corollaire) permet de montrer l'existence de codes avec certaines propriétés. Ces résultats seront utiles au chapitre 3.

Théorème 2.7.1 (Gilbert-Varshamov)**.** *Soient $m, d \in \mathbb{N}$. Il existe un $[n, k, d]$-code où $k \geq n - m$ si*

$$\binom{n-1}{1} + \binom{n-1}{2} + \cdots + \binom{n-1}{d-2} < 2^m - 1 \ . \tag{2.48}$$

La preuve du théorème ci-dessus peut être trouvée dans plusieurs ouvrages de référence, par exemple dans [Ple98]. En réarrangeant les termes de l'inégalité (2.48) et en bornant supérieurement la somme de coefficients binomiaux par $2^{h(\frac{d}{n})n}$, on obtient le corollaire suivant.

Corollaire 2.7.1. *Soient $k, n, d \in \mathbb{N}$. Il existe un $[n, k, d]$-code linéaire si*

$$k < n - h\left(\frac{d}{n}\right) \cdot n \ .$$

11. Comme on n'utilisera que des codes correcteurs linéaires dans ce document, nous laisserons sous-entendu l'adjectif « linéaire ».

2.8 Permutations et le sous-espace symétrique

Nous dénotons par $\mathcal{S}_n$ le *groupe symétrique* sur n éléments, c'est-à-dire le groupe formé par les $n!$ bijections — ou *permutations* — sur l'ensemble $\{1, \ldots, n\}$. On définit l'action de $\mathcal{S}_n$ sur les objets mathématiques rencontrés dans cette thèse de la manière suivante. Soit Σ un ensemble fini quelconque et soit $x = x_1 \ldots x_n \in \Sigma^n$, alors $\pi(x) := x_{\pi^{-1}(1)} \ldots x_{\pi^{-1}(n)}$ pour tout $\pi \in \mathcal{S}_n$ où π^{-1} est l'inverse de π dans le groupe $\mathcal{S}_n$. Soient $\mathsf{A}_1, \ldots, \mathsf{A}_n$ des registres quantiques de même taille ($\mathcal{H}_{\mathsf{A}_1} \simeq \cdots \simeq \mathcal{H}_{\mathsf{A}_n} \simeq \mathcal{H}$) et soit $\pi \in \mathcal{S}_n$. On abuse légèrement de la notation et on utilise le même symbole π pour désigner la transformation unitaire qui agit sur $\mathcal{H}^{\otimes n}$ par

$$\pi |\phi_1\rangle_{\mathsf{A}_1} \otimes \cdots \otimes |\phi_n\rangle_{\mathsf{A}_n} = \left|\phi_{\pi^{-1}(1)}\right\rangle_{\mathsf{A}_1} \otimes \cdots \otimes \left|\phi_{\pi^{-1}(n)}\right\rangle_{\mathsf{A}_n} = |\phi_1\rangle_{\mathsf{A}_{\pi(1)}} \otimes \cdots \otimes |\phi_n\rangle_{\mathsf{A}_{\pi(n)}} \ . \tag{2.49}$$

L'équation ci-dessus illustre le fait qu'il est important de prendre en compte l'ordre dans lequel les registres sont présentés lorsqu'on travaille avec les permutations. L'action de $\pi \in \mathcal{S}_n$ sur un opérateur de densité $\rho \in \mathcal{D}(\mathcal{H}^{\otimes n})$ est bien sûr définie par $\pi \rho \pi^*$.

Le *sous-espace symétrique* de $\mathcal{H}^{\otimes n}$ est le sous-espace de $\mathcal{H}^{\otimes n}$ composé des vecteurs qui sont *invariants* sous l'action de $\pi \in \mathcal{S}_n$, c'est-à-dire des vecteurs $|\phi\rangle \in \mathcal{H}^{\otimes n}$ tels que $\pi|\phi\rangle = |\phi\rangle$ pour tout $\pi \in \mathcal{S}_n$. On dénote ce sous-espace $\mathrm{Sym}^n(\mathcal{H})$. Bien sûr, tous les vecteurs invariants sous les permutations appartiennent au sous-espace symétrique, mais ce n'est pas vrai en général lorsqu'il s'agit des opérateurs invariants sous les permutations, c'est-à-dire que les opérateurs $A \in L(\mathcal{H}^{\otimes n})$ qui satisfont

$$\pi A \pi^* = A$$

n'ont pas nécessairement support dans $\mathrm{Sym}^n(\mathcal{H})$. Un exemple d'un tel opérateur invariant sous les permutations, mais qui n'a pas support dans le sous-espace symétrique est $\mathbb{1}_{\mathcal{H}^{\otimes n}}$. Par contre, les opérateurs de densité qui sont invariants sous les permutations admettent une purification dans le sous-espace symétrique d'un plus grand espace de Hilbert.

Proposition 2.8.1 ([Ren05, CKMR07])**.** *Pour tout opérateur de densité $\rho \in \mathcal{D}(\mathcal{H}^{\otimes n})$ invariant sous les permutations, il existe un état pur $|\psi\rangle \in \mathrm{Sym}^n(\mathcal{H}' \otimes \mathcal{H})$ où $\mathcal{H} \simeq \mathcal{H}'$ tel que $\mathrm{tr}_{\mathcal{H}'^{\otimes n}}(|\psi\rangle\langle\psi|) = \rho$.*

Il existe plusieurs manières de définir le projecteur sur le sous-espace symétrique. Nous nous servirons de la formulation suivante qui sera très utile au chapitre 4.

Proposition 2.8.2 ([Ren10, Ren05])**.** *Soit $\mathcal{H}$ un espace de Hilbert à dimension d. Le projecteur sur le sous-espace symétrique $\mathrm{Sym}^n(\mathcal{H})$ peut s'écrire comme*

$$\mathbb{1}_{\mathrm{Sym}^n(\mathcal{H})} := c_{n,d} \int |\theta\rangle\langle\theta|^{\otimes n} d|\theta\rangle \tag{2.50}$$

où $d|\theta\rangle$ *est la* mesure uniforme sphérique *sur l'ensemble des états purs de* $\mathcal{H}$ *et où* $c_{n,d} := \binom{n+d-1}{n} \leq (n+1)^{d-1}$ *est la dimension de* $\mathrm{Sym}^n(\mathcal{H})$.

L'opérateur présenté dans l'équation (2.50) ci-dessus requiert un peu plus d'explications. Sans trop entrer dans les détails, la mesure $d|\theta\rangle$ est définie comme l'unique mesure sur $\mathcal{H}$ qui est à la fois normalisée ($\int d|\theta\rangle = 1$) et invariante sous les transformations unitaires ($dU|\theta\rangle = d|\theta\rangle$). Celle-ci peut être interprétée comme une distribution de probabilité uniforme sur l'espace des états purs sur $\mathcal{H}$. Ainsi l'opérateur de l'équation (2.50) peut être interprété comme la valeur espérée de $X^{\otimes n}$ où X est une variable aléatoire qui « prend la valeur $|\theta\rangle\langle\theta|$ avec probabilité $d|\theta\rangle$ ». Bien sûr, cette interprétation ne correspond pas exactement à la réalité, mais donne une intuition suffisante sur les objets du type de (2.50). Les détails sur comment définir la mesure $d|\theta\rangle$ et les intégrales de la forme de (2.50) peuvent être trouvés dans [Wat17].

Pour les fins de cette thèse, les seules propriétés de (2.50) qui nous intéressent sont sa linéarité, c'est-à-dire que pour tout super-opérateur $\mathcal{E}$ sur $\mathcal{H}^{\otimes n}$, $\mathcal{E}(\int |\theta\rangle\langle\theta|^{\otimes n} d|\theta\rangle) = \int \mathcal{E}(|\theta\rangle\langle\theta|^{\otimes n}) d|\theta\rangle$, et que la mesure $d|\theta\rangle$ est normalisée, ce qui implique $\mathrm{tr}(\int |\theta\rangle\langle\theta|^{\otimes n} d|\theta\rangle) = \int \mathrm{tr}(|\theta\rangle\langle\theta|^{\otimes n}) d|\theta\rangle = \int d|\theta\rangle = 1$. Remarquons finalement que, si on prend la trace partielle de l'espace $\mathcal{H}'^{\otimes n}$ du projecteur sur l'espace symétrique $\mathrm{Sym}^n(\mathcal{H}' \otimes \mathcal{H})$, on obtient un opérateur de la forme

$$\mathrm{tr}_{\mathcal{H}'^{\otimes n}} \left(c_{n,d} \int |\theta\rangle\langle\theta|^{\otimes n} d|\theta\rangle \right) = c_{n,d} \int \theta^{\otimes n} d\theta \tag{2.51}$$

où $d\theta$ est une mesure normalisée sur l'ensemble des opérateurs de densité de $\mathcal{H}$ [ZS01].

2.9 Autres outils et définitions

On dit d'un opérateur $\tilde{\rho}_{\mathsf{A}} \in \mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{A}})$ qu'il est *post-sélectionné* du registre B de $\rho_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ s'il existe un élément de POVM $0 \leq E_{\mathsf{B}} \leq \mathbb{1}_{\mathsf{B}}$ tel que $\tilde{\rho}_{\mathsf{A}} = \mathrm{tr}_{\mathsf{A}}((\mathbb{1}_{\mathsf{A}} \otimes E_{\mathsf{B}})\rho_{\mathsf{AB}})$. La remarque suivante entre opérateur réduit et opérateur post-sélectionné nous sera utile.

Remarque 2.9.1. Soit $\rho_{\mathsf{AB}} \in \mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ un opérateur positif semi-défini sur les registres AB et soit $0 \leq E_{\mathsf{B}} \leq \mathbb{1}_{\mathsf{B}}$ un opérateur positif semi-défini agissant sur le registre B. Alors

$$\mathrm{tr}_{\mathsf{B}}\left((\mathbb{1}_{\mathsf{A}} \otimes E_{\mathsf{B}})\rho_{\mathsf{AB}}\right) \leq \mathrm{tr}_{\mathsf{B}}\left(\rho_{\mathsf{AB}}\right) \quad .$$

Démonstration. Il suffit de montrer que $\langle a| \mathrm{tr}_{\mathsf{B}}((\mathbb{1}_{\mathsf{A}} \otimes E_{\mathsf{B}})\rho_{\mathsf{AB}})|a\rangle \leq \langle a| \mathrm{tr}_{\mathsf{B}}(\rho_{\mathsf{AB}})|a\rangle$ pour tout $|a\rangle \in \mathcal{H}_{\mathsf{A}}$.

Soit dont $|a\rangle \in \mathcal{H}_{\mathsf{A}}$, alors

$$\begin{aligned}\langle a|\operatorname{tr}_{\mathsf{B}}\left((\mathbb{1}_{\mathsf{A}}\otimes E_{\mathsf{B}})\rho_{\mathsf{AB}}\right)|a\rangle &= \operatorname{tr}\left((|a\rangle\langle a|_{\mathsf{A}}\otimes E_{\mathsf{B}})\rho_{\mathsf{AB}}\right)\\ &= \langle a|_{\mathsf{A}}\operatorname{tr}_{\mathsf{B}}\left(\rho_{\mathsf{AB}}\right)|a\rangle_{\mathsf{A}}\cdot\operatorname{tr}\left(E_{\mathsf{B}}\rho_{\mathsf{B}}^{a}\right) \qquad (\rho_{\mathsf{B}}^{a}:=\operatorname{tr}_{\mathsf{A}}\left((|a\rangle\langle a|_{\mathsf{A}}\otimes\mathbb{1}_{\mathsf{B}})\rho_{\mathsf{AB}}\right))\\ &\leq \langle a|_{\mathsf{A}}\operatorname{tr}_{\mathsf{B}}\left(\rho_{\mathsf{AB}}\right)|a\rangle_{\mathsf{A}}\end{aligned}$$

car $\operatorname{tr}(E_{\mathsf{B}}\rho_{\mathsf{B}}^{a})\leq 1$. □

Une conséquence de la remarque ci-dessus est que si $\mathcal{E}_{\mathsf{B}}$ est un CPTN sur le registre B, alors la relation

$$\operatorname{tr}_{\mathsf{B}}\left((\mathrm{id}_{A}\otimes\mathcal{E}_{\mathsf{B}})(\sigma_{\mathsf{AB}})\right)\leq\sigma_{\mathsf{B}}$$

découle directement de la remarque 2.9.1 en considérant la représentation de Kraus de $\mathcal{E}_{\mathsf{B}}$ (voir théorèmes 2.3.2 et 2.3.3).

L'observation suivante montre qu'il y a une relation forte entre les opérateurs post-sélectionnés et les opérateurs bornés supérieurement.

Proposition 2.9.1. *Soit $c\geq 0$ et soient $\rho_{\mathsf{A}},\sigma_{\mathsf{A}}\in\mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{A}})$. Alors $\rho_{\mathsf{A}}\leq c\cdot\sigma_{\mathsf{A}}$ si et seulement si pour toute purification $|\sigma_{\mathsf{R}_1\mathsf{A}}\rangle$ de σ_{A} et $|\rho_{\mathsf{R}_2\mathsf{A}}\rangle$ de ρ_{A}, il existe un opérateur linéaire $A_{\mathsf{R}_1\to\mathsf{R}_2}$ tel que $A_{\mathsf{R}_1}^{*}A_{\mathsf{R}_1}\leq\mathbb{1}_{\mathsf{R}_1}$ et*

$$|\rho_{\mathsf{R}_2\mathsf{A}}\rangle=\sqrt{c}\cdot(A_{\mathsf{R}_1\to\mathsf{R}_2}\otimes\mathbb{1}_{\mathsf{A}})|\sigma_{\mathsf{R}_1\mathsf{A}}\rangle \tag{2.52}$$

Démonstration. Commençons avec la direction facile de la preuve. Soit $|\sigma_{\mathsf{R}_1\mathsf{A}}\rangle$ une purification de σ_{A}, soit $|\rho_{\mathsf{R}_2\mathsf{A}}\rangle$ une purification de ρ_{A} et soit $A_{\mathsf{R}_1\to\mathsf{R}_2}$ qui satisfait (2.52). Alors, par la remarque 2.9.1, ρ_{A} satisfait

$$\rho_{\mathsf{A}}=\operatorname{tr}_{\mathsf{R}_2}\left(\rho_{\mathsf{R}_2\mathsf{A}}\right)=c\cdot\operatorname{tr}_{\mathsf{R}_1}\left((A_{\mathsf{R}_1\to\mathsf{R}_2}^{*}A_{\mathsf{R}_1\to\mathsf{R}_2}\otimes\mathbb{1}_{\mathsf{A}})\sigma_{\mathsf{R}_1\mathsf{A}}\right)\leq c\cdot\operatorname{tr}_{\mathsf{R}_1}\left(\sigma_{\mathsf{R}_1\mathsf{A}}\right)=c\cdot\sigma_{\mathsf{A}}\ .$$

Pour la direction opposée, écrivons σ_{A} comme $\sigma_{\mathsf{A}}=\frac{1}{c}(\rho_{\mathsf{A}}+\tilde{\sigma}_{\mathsf{A}})$ où $\tilde{\sigma}_{\mathsf{A}}:=c\cdot\sigma_{\mathsf{A}}-\rho_{\mathsf{A}}\geq 0$. Soit $|\rho_{\mathsf{R}_2\mathsf{A}}\rangle$ une purification arbitraire de ρ_{A} et soit $|\tilde{\sigma}_{\mathsf{R}_2\mathsf{A}}\rangle$ une purification de $\tilde{\sigma}_{\mathsf{A}}$ qui vit dans le même espace. Alors considérons la purification suivante de σ_{A} : $|\sigma_{\mathsf{R}'\mathsf{R}_2\mathsf{A}}\rangle:=\sqrt{\frac{1}{c}}(|0\rangle_{\mathsf{R}'}|\rho_{\mathsf{R}_2\mathsf{A}}\rangle+|1\rangle_{\mathsf{R}'}|\tilde{\sigma}_{\mathsf{R}_2\mathsf{A}}\rangle)$. Soit $|\sigma_{\mathsf{R}_1\mathsf{A}}\rangle$ une purification arbitraire de σ_{A} et définissons $A_{\mathsf{R}_1\to\mathsf{R}_2}:=(\langle 0|_{\mathsf{R}'}\otimes\mathbb{1}_{\mathsf{R}_2})V_{\mathsf{R}_1\to\mathsf{R}'\mathsf{R}_2}$ où $V_{\mathsf{R}_1\to\mathsf{R}'\mathsf{R}_2}$ est une isométrie qui transforme $|\sigma_{\mathsf{R}_1\mathsf{A}}\rangle$ en $|\sigma_{\mathsf{R}'\mathsf{R}_2\mathsf{A}}\rangle$. Alors

$$(A_{\mathsf{R}_1\to\mathsf{R}_2}\otimes\mathbb{1}_{\mathsf{A}})|\sigma_{\mathsf{R}_1\mathsf{A}}\rangle=(\langle 0|_{\mathsf{R}'}\otimes\mathbb{1}_{\mathsf{R}})|\sigma_{\mathsf{R}'\mathsf{R}_2\mathsf{A}}\rangle=\sqrt{\frac{1}{c}}|\rho_{\mathsf{R}_2\mathsf{A}}\rangle\ .$$ □

La proposition suivante est une généralisation d'un lemme qu'on peut trouver dans [BF10], qui est lui-même inspiré d'un résultat de [Ren05]. Une conséquence directe de cette proposition est qu'une superposition d'un petit nombre d'états purs peut être approximée par une mixture de ces mêmes états.

Proposition 2.9.2. *Soit $\{|\psi_i\rangle\}_{i\in\Sigma} \subset \mathcal{H}$ une famille de vecteurs indexée par un ensemble fini Σ. Définissons les opérateurs*

$$\rho = \sum_{i,j\in\Sigma} |\psi_i\rangle\langle\psi_j| \text{ et } \rho^{mix} = \sum_{i\in\Sigma} |\psi_i\rangle\langle\psi_i| \ .$$

Alors, $\rho \leq |\Sigma| \cdot \rho^{mix}$.

Démonstration. Il suffit de montrer que $\langle a| \left(|\Sigma| \cdot \rho^{mix}\right) |a\rangle \geq \langle a|\rho|a\rangle$ pour tout $|a\rangle \in \mathcal{H}$. Considérons la chaine d'(in)égalités suivante :

$$\begin{aligned}|\Sigma|\langle a|\rho^{mix}|a\rangle &= |\Sigma|\langle a| \left(\sum_{i\in\Sigma} |\psi_i\rangle\langle\psi_i|\right) |a\rangle = |\Sigma| \sum_{i\in\Sigma} |\langle a|\psi_i\rangle|^2 \\ &\geq \left|\sum_{i\in\Sigma} \langle a|\psi_i\rangle\right|^2 = \left(\sum_{i\in\Sigma} \langle a|\psi_i\rangle\right) \left(\sum_{j\in\Sigma} \langle\psi_j|a\rangle\right) = \langle a| \left(\sum_{i,j\in\Sigma} |\psi_i\rangle\langle\psi_j|\right) |a\rangle = \langle a|\rho|a\rangle\end{aligned}$$

où la seule inégalité dans l'équation précédente découle de l'inégalité de Cauchy-Schwarz $|\langle\varphi|\psi\rangle|^2 \leq \langle\varphi|\varphi\rangle\langle\psi|\psi\rangle$ avec $|\varphi\rangle = \sum_{i\in\Sigma} |i\rangle$ et $|\psi\rangle = \sum_{i\in\Sigma} \langle a|\psi_i\rangle|i\rangle$. □

La définition suivante est une généralisation de la sphère de Hamming aux états quantiques. Elle capture une notion de « distance » distincte de celles présentées à la section 2.3.7.

Définition 2.9.1 (Sphère de Hamming quantique)**.** Soient $n \in \mathbb{N}$, $|\Psi\rangle \in \mathcal{H}^{\otimes n}$ et $r \in [n]$. Nous définissons la *sphère de Hamming quantique* de rayon r autour de $|\Psi\rangle$, $\Delta_r(|\Psi\rangle)$, comme le sous-espace engendré par tous les vecteurs de la forme $U|\Psi\rangle$ pour toute transformation unitaire U qui agit comme l'identité sur au moins $n - r$ sous-systèmes.

Pour le cas spécial $|\Psi\rangle = |\nu\rangle^{\otimes n}$, la sphère de Hamming quantique peut être définie par

$$\Delta_r(|\nu\rangle^{\otimes n}) = \text{span}\{\pi(|\nu\rangle^{\otimes n-r} \otimes |u\rangle) \ : \ |u\rangle \in \mathcal{B}, \pi \in \mathcal{S}_n\}$$

où $\mathcal{B}$ est une base quelconque de $\mathcal{H}^{\otimes r}$.

Le projecteur sur la sphère de Hamming de rayon r autour d'un état i.i.d. $|\nu\rangle^{\otimes n} \in \mathcal{H}_{\mathsf{A}_1} \otimes \cdots \otimes \mathcal{H}_{\mathsf{A}_n}$ peut être écrit comme

$$\mathbb{P}^{r,|\nu\rangle}_{\mathsf{A}^n} = \sum_{E\subseteq[n] \,:\, |E|\leq r} \left(\bigotimes_{i\in E} (\mathbb{1} - |\nu\rangle\langle\nu|)_{\mathsf{A}_i} \bigotimes_{i\notin E} |\nu\rangle\langle\nu|_{\mathsf{A}_i}\right) \ .$$

Chapitre 3

Stratégies adaptées et non adaptées dans le monde quantique

Ce chapitre fait état d'une partie de mes travaux réalisés en collaboration avec Louis Salvail, Frédéric Dupuis et Serge Fehr. Ces travaux ont été publiés dans les actes de conférence de CRYPTO 2016 [DFLS16a] et ont également été présentés à QCrypt 2016 [DFLS16b].

3.1 Introduction

3.1.1 Adversaires adaptés et non adaptés

Considérons le scénario où deux participants, Alice et Bob, veulent réaliser une tâche cryptographique à l'aide d'un protocole quantique. Nous allons comparer deux types d'attaques contre un protocole quantique. Dans le premier, l'adversaire dispose d'information auxiliaire corrélée avec l'état du participant honnête. Dans le second, l'état de l'adversaire est complètement indépendant de celui du participant honnête. On utilisera l'adjectif *adapté*, par opposition à *non adapté*, afin de désigner un adversaire ayant accès à de l'information auxiliaire corrélée avec le participant honnête. Cette information peut être classique, et ainsi corrélée classiquement, mais aussi quantique, auquel cas la corrélation peut prendre la forme d'intrication entre les registres des deux participants. Dans ce chapitre, nous allons établir une relation entre les adversaires adaptés et non adaptés pour des protocoles quantiques, et ainsi profiter du fait que les adversaires non adaptés sont généralement beaucoup plus faciles à analyser.

Il est clair qu'un adversaire adapté possède un avantage indéniable par rapport à un adversaire non adapté. Cet avantage est toutefois limité par la *quantité* et la *qualité* de l'information auxiliaire dont dispose l'adversaire. Dans le cas d'un protocole et d'un adversaire tous deux classiques, il est possible de formaliser cette limite par l'argument suivant. Supposons qu'un adversaire adapté dispose de n bits d'information auxiliaire, alors cette information ne peut pas augmenter la probabilité de réussir son attaque, par rapport à un adversaire non adapté, par plus qu'un facteur de 2^n. En effet, une stratégie possible pour un adversaire non adapté est de *deviner* les n bits de cette information auxiliaire et d'appliquer la stratégie de l'adversaire adapté correspondant à cette valeur de l'information auxiliaire. Il s'en suit que

$$P_{\text{succ}}^{\text{NA}} \geq 2^{-n} P_{\text{succ}}^{\text{A}} \ ,$$

où $P_{\text{succ}}^{\text{A}}$ et $P_{\text{succ}}^{\text{NA}}$ représentent les probabilités de succès maximales pour les adversaires adaptés et non adaptés, respectivement. Ceci donne lieu à la relation

$$P_{\text{succ}}^{\text{A}} \leq 2^n P_{\text{succ}}^{\text{NA}} \tag{3.1}$$

en réarrangeant les termes. Bien qu'il s'agisse d'une augmentation exponentielle de la probabilité de succès, cette relation entre adversaires adaptés et non adaptés, que nous nommons relation *A-vs-NA*, donne une borne non triviale dès qu'on peut contrôler la taille de l'information auxiliaire et que $P_{\text{succ}}^{\text{NA}}$ est assez petit (négligeable).

3.1.2 Aperçu des résultats

Dans ces travaux, nous considérons le cas où le protocole cryptographique, et donc aussi l'information auxiliaire, peuvent être quantiques. Une question naturelle à se poser est de savoir si une relation similaire à (3.1) existe encore lorsque les adversaires sont quantiques. Une réponse simple à cette question est de considérer l'équivalent quantique de l'argument que nous avons utilisé au paragraphe précédent pour borner l'avantage que confère de l'information auxiliaire classique. L'analogue le plus près de *deviner* l'information auxiliaire dans le monde quantique est de remplacer les n qubits d'information auxiliaire par un registre quantique dans l'état complètement mixte $\frac{\mathbb{1}}{2^n}$. Supposons qu'Alice joue le rôle de l'adversaire et qu'elle détient de l'information auxiliaire contenue dans le registre A corrélé quantiquement avec le registre B de Bob. Si cette corrélation est capturée par la matrice de densité ρ_{AB}, alors il est possible de montrer [1] que

$$\rho_{\mathsf{AB}} \leq 2^{2n} \frac{\mathbb{1}_{\mathsf{A}}}{2^n} \otimes \rho_{\mathsf{B}} \tag{3.2}$$

lorsque $\dim \mathcal{H}_{\mathsf{A}} = 2^n$. Il en découle que la relation $P_{\text{succ}}^{\text{A}} \leq 2^{2n} P_{\text{succ}}^{\text{NA}}$ tient pour les adversaires quantiques, puisqu'on peut remplacer l'état conjoint ρ_{AB} par l'état non corrélé $\frac{\mathbb{1}_{\mathsf{A}}}{2^n} \otimes \rho_{\mathsf{B}}$ en payant un prix de 2^{2n}

1. Voir par exemple [BCR11, Lemme B.9].

dans la probabilité de succès. En effet, pour tout élément de POVM E_{AB} décrivant un résultat favorable à l'adversaire à la suite d'un protocole culminé d'une mesure, la borne (3.2) implique que

$$\operatorname{tr}\left(E_{\mathsf{AB}}\ \rho_{\mathsf{AB}}\right) \leq 2^{2n} \operatorname{tr}\left(E_{\mathsf{AB}}\left(\frac{\mathbb{1}_{\mathsf{A}}}{2^n} \otimes \rho_{\mathsf{B}}\right)\right) \quad .$$

La borne supérieure de (3.2) est optimale, car, pour certains états ρ_{AB} (en particulier pour l'état pur $2^{-n/2}\sum_{x\in\{0,1\}^n} |x\rangle_{\mathsf{A}}|x\rangle_{\mathsf{B}}$), le plus petit λ tel que $\rho_{\mathsf{AB}} \leq 2^{\lambda}\frac{\mathbb{1}_{\mathsf{A}}}{2^n} \otimes \rho_{\mathsf{B}}$ est $\lambda = 2\dim(\mathcal{H}_{\mathsf{A}})$. Donc avec cette approche, le facteur supplémentaire de 2 dans l'exposant est inévitable.

Le résultat principal de ce chapitre (Théorème 3.2.1, section 3.2) est de montrer qu'il est possible de faire une analyse plus raffinée des stratégies adaptées et non adaptées dans un contexte quantique. Nous montrons que dans un contexte général, mais précis, la quantité $P^{\mathrm{A}}_{\mathrm{succ}}$ est bornée par

$$P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^{\mathrm{I}^{\mathrm{acc}}_{\mathrm{max}}(\mathsf{B};\mathsf{A})_{\rho}} P^{\mathrm{NA}}_{\mathrm{succ}} \quad , \tag{3.3}$$

où $\mathrm{I}^{\mathrm{acc}}_{\mathrm{max}}(\mathsf{B};\mathsf{A})_{\rho}$ est une nouvelle mesure d'information quantique qui détermine la *qualité* de la corrélation entre A et B. En particulier $\mathrm{I}^{\mathrm{acc}}_{\mathrm{max}}(\mathsf{B};\mathsf{A})_{\rho}$ est bornée supérieurement par $\mathrm{H}_0(\mathsf{A})$, une mesure d'information introduite à la section 2.5 et dont la valeur est d'au plus le nombre de qubits n du registre quantique A. Nous retrouvons donc la relation classique $P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^n P^{\mathrm{NA}}_{\mathrm{succ}}$ comme cas particulier de la relation (3.3), mais cette fois-ci dans un contexte d'information quantique.

Plus précisément, le contexte que nous considérons peut être capturé par le « jeu » suivant, illustré à la figure 3.1. Ce jeu est joué par Alice et Bob qui détiennent respectivement les registres A et B d'un état ρ_{AB}. Le jeu comprend également une famille de mesures $\{\mathcal{N}^j\}_{j\in\mathcal{J}}$ sur le registre B où chaque mesure $\mathcal{N}^j$ a deux résultats possibles : « succès » ou « échec ». Le jeu est joué ainsi : Alice choisit un indice $j \in \mathcal{J}$ et le communique à Bob qui mesure son registre avec la mesure $\mathcal{N}^j$. Alice gagne ce jeu si le résultat de la mesure de Bob est « succès ». Alice utilise une stratégie adaptée si elle tire avantage du registre A corrélé avec le registre de Bob en le mesurant. Une stratégie non adaptée consiste à choisir j sans recourir au registre A. Ce jeu, bien que conceptuellement simple, représente un scénario que l'on retrouve couramment dans des protocoles cryptographiques quantiques et où gagner le jeu correspond à briser le protocole. Notre résultat principal consiste à montrer que pour un tel jeu, la probabilité de gagner par une stratégie adaptée est limitée par la relation $P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^{\mathrm{I}^{\mathrm{acc}}_{\mathrm{max}}(\mathsf{B};\mathsf{A})_{\rho}} P^{\mathrm{NA}}_{\mathrm{succ}}$.

3.1.3 Exemples

Comme premier indice de l'utilité de notre résultat, il est possible de déterminer une borne inférieure sur la quantité, ou plutôt la *qualité* (mesurée par $\mathrm{I}^{\mathrm{acc}}_{\mathrm{max}}(\mathsf{B};\mathsf{A})_{\rho}$), d'intrication qu'un adversaire requiert pour exécuter l'attaque générique [May97] sur les protocoles quantiques de mise en gage. Considérons

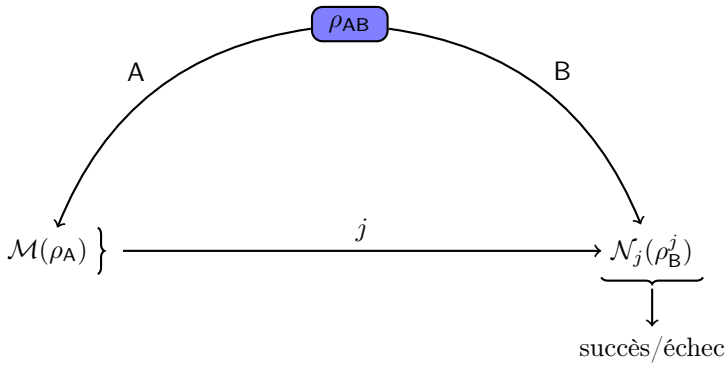


FIGURE 3.1 – Le *jeu* pour lequel nous avons montré la relation $P_{\text{succ}}^{\text{A}} \leq 2^{\text{I}_{\max}^{\text{acc}}(\mathsf{B};\mathsf{A})_\rho} P_{\text{succ}}^{\text{NA}}$ où $\{\mathcal{N}_j\}_{j\in\mathcal{J}}$ est une famille de mesures à deux résultats sur le registre de Bob et où $\mathcal{M}$ est une mesure du côté d'Alice qui produit la valeur j qu'elle envoie à Bob. Alice gagne le jeu si la mesure de Bob produit le résultat « succès ».

un protocole de mise en gage quelconque où Alice se met en gage à Bob et où la phase d'ouverture du protocole se résume à Alice qui envoie une chaine classique j et Bob qui applique une procédure de vérification $\mathcal{N}_j$ qui peut être représentée par un POVM $\{E_{\text{acc}}^j, E_{\text{rej}}^j\}$ où E_{acc}^j correspond à l'évènement où Bob accepte l'ouverture j et E_{rej}^j à celui où Bob rejette l'ouverture. Dans l'attaque générique, Alice se met toujours en gage à la valeur 0 de manière honnête, mais en purifiant toutes ses actions, et applique une transformation sur son registre si elle souhaite changer sa mise en gage pour la valeur 1. Si l'état conjoint après la phase de mise en gage (où Alice s'est engagé à 0) est ρ_{AB}, alors la probabilité maximale qu'Alice puisse ouvrir un 1 sans avoir recours à sa mémoire quantique est $P_{\text{succ}}^{\text{NA}} = \max_j \text{tr}((\mathbb{1}_{\mathsf{A}} \otimes E_{\text{acc}}^j)\rho_{\mathsf{AB}})$ où le maximum est sur toutes les chaines classiques j qui ouvrent la valeur 1. Si Alice détient un registre A intriqué avec B, notre relation A-vs-NA quantique implique que $\text{I}_{\max}^{\text{acc}}(\mathsf{B};\mathsf{A})_\rho$ doit être proportionnel à $-\log P_{\text{succ}}^{\text{NA}}$ pour qu'Alice ait une probabilité constante de changer la valeur de sa mise en gage.

Un second exemple de la versatilité de notre résultat est qu'il implique immédiatement la *règle de chaine* pour la min-entropie d'une variable classique avec information auxiliaire quantique (voir équation (2.46) et proposition 2.5.1 des préliminaires). En effet, si on considère un *jeu de devinette* où Alice doit déterminer la valeur du registre *classique* B à partir du registre A de $\rho_{\mathsf{AB}} = \sum_b P_B(b)\rho_{\mathsf{A}}^b \otimes |b\rangle\langle b|_{\mathsf{B}}$. Ce jeu est un cas spécial de celui que nous avons décrit plus haut où le registre de Bob est classique et où la mesure $\mathcal{N}^j$ consiste à tester si ce registre classique contient la valeur j, autrement dit, celle-ci correspond au POVM formé des opérateurs $E_0^j = |j\rangle\langle j|$ et $E_1^j = \mathbb{1} - |j\rangle\langle j|$. Par les propriétés de la min-entropie énoncées à la section 2.5, les probabilités de succès adaptées et non adaptées pour ce jeu correspondent respectivement à $P_{\text{succ}}^{\text{A}} = 2^{-\text{H}_\infty(\mathsf{B}|\mathsf{A})}$ et $P_{\text{succ}}^{\text{NA}} = 2^{-\text{H}_\infty(\mathsf{B})}$. Alors

$$P_{\text{succ}}^{\text{A}} \leq 2^{\text{I}_{\max}^{\text{acc}}(\mathsf{B};\mathsf{A})_\rho} P_{\text{succ}}^{\text{NA}} \implies 2^{-\text{H}_\infty(\mathsf{BA})} \leq 2^{\text{H}_0(\mathsf{A})} 2^{-\text{H}_\infty(\mathsf{B})} , \tag{3.4}$$

et on obtient ainsi la règle de chaine en prenant le logarithme de base 2 de chaque côté de l'inégalité.

Les exemples ci-dessus, bien que simples, démontrent comment notre résultat peut être pratique pour démontrer la sécurité de protocoles cryptographiques quantiques. Mais le vrai potentiel de notre résultat réside dans le fait que les stratégies quantiques adaptées sont beaucoup plus difficiles à analyser que les stratégies non adaptées. Ainsi, il fournit un outil puissant au cryptographe quantique : tant qu'il est possible d'avoir un certain contrôle sur l'information auxiliaire, il est suffisant de restreindre l'analyse aux adversaires non adaptés.

3.1.4 Applications

Nous démontrons l'utilité de notre résultat principal en l'utilisant comme outil pour résoudre deux questions ouvertes. Dans chacun des cas, la preuve nous demande de démontrer la sécurité d'un protocole quantique de mise en gage et le fait que l'adversaire détienne de l'information auxiliaire quantique corrélée d'une quelconque manière avec le participant honnête empêche une analyse directe. Nous évitons ce problème en analysant une variante non adaptée de l'adversaire et en y appliquant notre relation A-vs-NA.

La complétude de la primitive 1CC dans le modèle UC quantique

Comme première application, nous proposons un nouveau protocole quantique de mise en gage dans la section 3.3 dont la sécurité repose sur l'hypothèse d'un protocole implémentant la primitive cryptographique 1CC (voir Fig. 2.1 à la section 2.4). Puisque la primitive de mise en gage BC est universelle pour le calcul sûr à deux partis dans le monde quantique, notre réduction de BC à 1CC implique que la primitive 1CC l'est aussi. Cette réduction répond à la principale question ouverte de [FKS+13] où les auteurs prouvent qu'il existe une loi « zero/xor/one » qui régit la puissance cryptographique des primitives dans le monde quantique. Cette loi stipule que toute primitive appartient à une de trois catégories mutuellement exclusives. Une primitive est soit

1. complète (« one »), auquel cas elle permet de réaliser toute autre primitive de manière sûre,
2. triviale (« zero »), auquel cas elle peut être réalisée de manière sûre par un protocole quantique sans hypothèse supplémentaire,
3. ou appartient à une classe de primitives équivalentes à un échange instantané de messages — ou encore à la primitive XOR.

Une pièce importante manquait toutefois à la caractérisation précédente des primitives cryptographiques ; les auteurs de [FKS+13] ont été incapables de montrer que cette loi s'applique à une famille de primitives

assez puissantes pour réaliser 1CC, mais trop faibles pour réaliser 2CC. Nous complétons cette caractérisation en montrant que 1CC appartient à la classe des primitives complètes dans un monde quantique.

La sécurité du protocole de mise en gage BCJL dans le modèle à mémoire bornée.

Comme deuxième application de notre relation A-vs-NA, nous considérons une classe générale de protocoles de mise en gage *non interactifs*. Nous montrons dans la section 3.4 que la sécurité de ces protocoles contre les adversaires sans mémoire quantique implique leur sécurité dans une variante du modèle à mémoire bornée où, en plus de borner la mémoire de l'adversaire, on restreint également ses mesures à des mesures projectives. Cette restriction est en partie justifiée par le fait que les mesures les plus générales nécessitent de la mémoire quantique additionnelle sous forme de système auxiliaire pour être réalisées par un circuit quantique. La quantité de mémoire adversarielle qu'un protocole particulier peut tolérer dépend de la probabilité de tricher d'un adversaire sans mémoire [2].

Pour illustrer la pertinence de l'application ci-dessus, nous revisitons la sécurité du protocole de mise en gage proposé en 1993 par Brassard, Crépeau, Josza et Langlois [BCJL93]. Ce protocole fut proposé à l'époque comme candidat pour un protocole inconditionnellement sûr — avant que cette tâche soit démontrée impossible [May97, LC98] — mais n'avait depuis reçu aucun traitement rigoureux basé sur des hypothèses et des techniques modernes. Nous utilisons la réduction générale mentionnée au paragraphe précédent pour montrer que le protocole BCJL est sûr dans la variante du modèle à mémoire bornée que nous considérons.

3.1.5 Travaux précédents

Classification des primitives cryptographiques

C'est un fait bien connu dans la communauté cryptographique qu'il est impossible de réaliser le calcul sûr à deux participants de manière inconditionnellement sûre. Ainsi une question naturelle à se poser est : quelles sont les hypothèses minimales nécessaires pour y parvenir ? Une réponse possible à cette question est d'identifier les primitives cryptographiques les plus simples telles que, lorsqu'utilisées comme sous-routines par accès *boîte noire*, elles permettent de réaliser tout calcul biparti de manière sûre. Si une primitive satisfait cette propriété, on dit qu'elle est *universelle*. La plus connue de ces primitives est OT, montrée universelle par Kilian [Kil88]. Depuis, la puissance cryptographique de plusieurs primitives a été étudiée en plus de détail [Kil91, Kil00, MPR10, KMQ11b, MPR12, Kra13].

2. Nous avons déjà montré comment analyser la quantité d'intrication qui serait nécessaire pour attaquer un protocole de mise en gage avec l'attaque générique ; lorsqu'on considère des attaques *arbitraires*, la tâche est plus complexe.

Un résultat récent de Maji, Prabhakaran et Rosulek [MPR10] établit que dans le monde classique, toute primitive bipartite non triviale peut servir à implémenter une des quatre primitives suivantes : transfert équivoque (OT), mise en gage (BC), transfert sélectif à un bit (1CC) ou le transfert instantané des entrées d'Alice et Bob (équivalent à calculer la fonctionnalité XOR). Autrement dit, pour n'importe quelle primitive $\mathcal{F}$ non triviale, il existe une primitive $\mathcal{G} \in \{\mathcal{F}_{\text{OT}}, \mathcal{F}_{\text{BC}}, \mathcal{F}_{1\text{CC}}, \mathcal{F}_{\text{XOR}}\}$ telle que $\mathcal{G} \sqsubseteq \mathcal{F}$. Ces primitives sont décrites à la section 2.4. Les auteurs utilisent cette réduction pour montrer que, sous l'hypothèse qu'il existe un protocole sûr pour transfert équivoque contre les adversaires semi-honnêtes polynomiaux [3], toute primitive cryptographique est soit triviale, soit complète. Ils désignent cette classification des primitives bipartites comme loi « *zero-one* ».

Le portrait se simplifie grandement lorsqu'on considère des protocoles quantiques. D'abord, la fonctionnalité BC peut être utilisée en accès boîte noire pour réaliser de manière sûre OT [BBCS91, Cré94, Unr10, BF10] sans hypothèse supplémentaire et est donc universelle. De plus, même la primitive transfert sélectif à deux bits (2CC) est universelle dans le monde quantique, tel que démontré par Fehr, Katz, Song, Zhou et Zikas [FKS+13]. Ces auteurs montrent ainsi qu'une loi « *zero/xor/one* » s'applique aux primitives bipartites dans le monde quantique, et ce sans hypothèse supplémentaire sur la puissance de l'adversaire. Il manquait cependant un élément important à cette classification : celle-ci s'applique à toutes les fonctionnalités, excepté celles qui permettent de réaliser le transfert sélectif à un bit (1CC), mais pas celui à deux bits (2CC). Il est en effet possible de montrer qu'il existe une hiérarchie infinie de primitives de type transfert sélectif dans le monde classique où chaque niveau de la hiérarchie, représenté par la taille de l'entrée, est strictement plus faible que le suivant :

$$\mathcal{F}_{1\text{CC}} \not\sqsubseteq \mathcal{F}_{2\text{CC}} \not\sqsubseteq \cdots \not\sqsubseteq \mathcal{F}_{m\text{CC}} \not\sqsubseteq \cdots \ .$$

Dans la section 3.3, nous complétons la classification des primitives bipartites dans le monde quantique en montrant que la primitive 1CC est universelle. Nous utilisons l'accès comme boîte noire à 1CC comme hypothèse pour construire un protocole quantique pour BC. Comme les classifications des primitives cryptographiques ci-haut concernent le modèle UC, nous utilisons le protocole de mise en gage que nous avons construit pour démontrer que 1CC est complète dans le modèle UC.

Protocole BCJL et modèle à mémoire bornée

Notre seconde application a également un riche passé. Le protocole de mise en gage BCJL mentionné plus haut est un protocole de mise en gage proposé en 1993 par Brassard, Crépeau, Jozsa, et Langlois [BCJL93]

3. L'hypothèse « sh-OT » suppose l'existence d'un protocole pour OT sûr dans le modèle à sécurité autonome contre les adversaires honnêtes, mais curieux (c'est-à-dire qui respectent le protocole, mais cherchent à en soutirer le maximum d'information), qui fonctionnent en temps polynomial.

comme un candidat pour un protocole de mise en gage inconditionnellement sûr. À l'époque, la mécanique quantique offrait de nouvelles possibilités pour la cryptographie, et tous les espoirs étaient permis. Toutefois, l'impossibilité de la mise en gage quantique fut démontrée par Mayers [May97], et indépendamment par Lo et Chau [LC98]. Le protocole BCJL présentait des idées novatrices pour l'époque, mais sa sûreté sous des hypothèses raisonnables n'avait pas été revisitée jusqu'à maintenant. Notre relation entre les adversaires adaptés et non adaptés nous permet de montrer la sûreté du protocole BCJL dans une version légèrement modifiée du modèle à mémoire bornée.

Le modèle à mémoire bornée est une hypothèse qui est faite sur les capacités de traitement de l'information quantique de l'adversaire [DFSS08, DFSS07, Sch07]. Au lieu de restreindre son temps de calcul et de s'en remettre à des hypothèses calculatoires, comme la difficulté de factoriser de grands nombres, on limite la *quantité* d'information quantique que l'adversaire peut garder en mémoire. Cette hypothèse est justifiée par le fait que le plus grand défi à la construction d'un ordinateur quantique est de préserver un état quantique de manière *cohérente* sur un moyen physique, c'est-à-dire sans que celui-ci soit perturbé par des interactions avec son environnement. En général, on suppose dans ce modèle que l'adversaire ne peut garder en mémoire qu'une fraction constante des particules échangées. Le modèle à mémoire bornée est maintenant réputé comme une hypothèse suffisante pour implémenter l'ensemble de la cryptographie, puisque des protocoles existent qui implémentent les primitives complètes OT et BC [DFSS08, Sch07] de manière sûre sous cette hypothèse.

Une hypothèse semblable à celle du modèle à mémoire bornée, et qui généralise cette dernière, est le modèle à mémoire *bruitée* [WST08, STW09, WCSL10, Sch10, KWW12]. Dans ce modèle, on ne fait aucune hypothèse sur la quantité de mémoire que l'adversaire détient, mais plutôt sur la *qualité* de celle-ci. Ce modèle suppose qu'à un certain point dans un protocole, du *bruit* sera appliqué sur la mémoire quantique de l'adversaire. Ce bruit est modélisé par un canal quantique (un CPTP) et il existe différents types de bruit auquel on pourrait soumettre la mémoire de l'adversaire. Le modèle à mémoire bruitée est également une hypothèse suffisante pour implémenter de manière sûre OT et BC [WST08, STW09, WCSL10, Sch10, KWW12] (pour les modèles de bruit adéquats). Récemment, un modèle unificateur de différents types de bruits quantiques fut proposé dans [KWW12].

3.2 Une relation A-vs-NA quantique

Nous considérons un *jeu* abstrait entre deux participants : Alice et Bob. Le jeu est paramétré par un état conjoint ρ_{AB} dont Alice et Bob détiennent respectivement les registres A et B, ainsi que par une famille $\mathbf{E} = \{E^j\}_{j\in\mathcal{J}}$ de mesures POVM $E^j = \{E^j_0, E^j_1\}$. Le jeu se joue comme suit : Alice annonce un

indice $j \in \mathcal{J}$ à Bob et Bob mesure son registre B avec le POVM E^j déterminé par j. Alice *gagne* si le résultat de la mesure est 1. On distingue entre les stratégies adaptées et non adaptées pour Alice : Alice est adaptée si elle effectue une mesure sur son registre A pour obtenir j et est non adaptée si elle ne se sert pas de son registre quantique. C'est ce qui motive les définitions suivantes.

Définition 3.2.1. Soit $\mathcal{J}$ un ensemble fini non vide, soit ρ_{AB} un état quantique biparti, et soit $\mathbf{E} = \{E^j\}_{j\in\mathcal{J}}$ une famille de mesures POVM à résultat binaire, où $E^j = \{E_0^j, E_1^j\}$ agit sur B. Alors, définissons

$$P_{\text{succ}}(\rho_{\mathsf{AB}}, \mathbf{E}) := \max_{\{F_j\}_j} \sum_{j\in\mathcal{J}} \text{tr}\Big(\big(F_j \otimes E_1^j\big)\rho_{\mathsf{AB}}\Big) \ , \tag{3.5}$$

où le maximum est sur toutes les mesures POVM $\{F_j\}_{j\in\mathcal{J}}$ agissant sur A. On nomme $P_{\text{succ}}(\rho_{\mathsf{AB}}, \mathbf{E})$ la *probabilité de succès adaptée*, et on nomme $P_{\text{succ}}(\rho_{\mathsf{B}}, \mathbf{E})$ la *probabilité de succès non adaptée*, où cette dernière probabilité correspond au cas spécial où le registre A est vide, auquel cas elle est égale à

$$P_{\text{succ}}(\rho_{\mathsf{B}}, \mathbf{E}) = \max_{j\in\mathcal{J}} \text{tr}\big(E_1^j\rho_{\mathsf{B}}\big) \ .$$

Si cela ne pose pas d'ambiguïté, c'est-à-dire si ρ_{AB} et $\mathbf{E}$ sont connus par le contexte, on écrit $P_{\text{succ}}^{\text{A}}$ et $P_{\text{succ}}^{\text{NA}}$ au lieu de $P_{\text{succ}}(\rho_{\mathsf{AB}}, \mathbf{E})$ et $P_{\text{succ}}(\rho_{\mathsf{B}}, \mathbf{E})$.

Pour être le plus général possible, nous considérons également la situation où Alice a accès à un second registre A' à la fois pour la stratégie adaptée et non adaptée, mais où elle a accès au registre A seulement pour la stratégie adaptée. Dans ce nouveau contexte, on peut comparer les stratégies complètement adaptées (ayant accès à A et A') aux stratégies *semi-adaptées* (ayant accès seulement à A'). Formellement, on considère dans ce cas un état triparti $\rho_{\mathsf{AA'B}}$ et on fait le lien entre $P_{\text{succ}}(\rho_{\mathsf{AA'B}}, \mathbf{E})$ et $P_{\text{succ}}(\rho_{\mathsf{A'B}}, \mathbf{E})$. Ces quantités sont bien définies, car le maximum dans la définition de P_{succ} est pris sur tous les mesures POVM agissant sur tous les registres sous le contrôle d'Alice.

Nous introduisons maintenant une nouvelle mesure d'information quantique, la *max-information accessible* $\text{I}_{\max}^{\text{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho$, qui nous permettra de faire le lien entre les stratégies adaptées et les stratégies semi- ou non adaptées dans notre résultat principal. Dans sa forme non conditionnelle $\text{I}_{\max}^{\text{acc}}(\mathsf{B};\mathsf{A})_\rho$, cette mesure correspond à une variante *accessible* (par une mesure) de la max-information $\text{I}_{\max}(\mathsf{B};\mathsf{A})_\rho$ introduite dans [BCR11]. Autrement dit, c'est la quantité de max-information qui peut être accédée par une mesure du côté d'Alice.

Définition 3.2.2. Soit $\rho_{\mathsf{AA'B}}$ un état quantique triparti. On définit la *max-information accessible* que le registre A détient à propos de B conditionné sur A' comme le plus petit nombre réel $\text{I}_{\max}^{\text{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho$ tel que pour toute mesure $\mathcal{M}_{\mathsf{AA'}\to\mathsf{X}}$ sur les registres AA', il existe une mesure $\mathcal{N}_{\mathsf{A'}\to\mathsf{X}}$ sur le registre A' telle que

$$\mathcal{M}_{\mathsf{AA'}}(\rho_{\mathsf{AA'B}}) \leq 2^{\text{I}_{\max}^{\text{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho}\mathcal{N}_{\mathsf{A'}}(\rho_{\mathsf{A'B}}) \ . \tag{3.6}$$

La version non conditionnelle $\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A})_\rho$ est définie naturellement en considérant A' comme étant trivial. La condition (3.6) ci-dessus coïncide alors avec

$$\mathcal{M}_{\mathsf{A}}(\rho_{\mathsf{AB}}) \leq 2^{\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A})_\rho}\sigma_{\mathsf{X}} \otimes \rho_{\mathsf{B}} \ , \tag{3.7}$$

pour une matrice de densité quelconque $\sigma_{\mathsf{X}} \in \mathcal{D}(\mathcal{H}_{\mathsf{X}})$ qui peut être interprétée comme le résultat d'une mesure $\mathcal{N}_{\mathbb{C}\to\mathsf{X}}$ sur un registre trivial.

Nous sommes maintenant prêts à énoncer et démontrer notre résultat principal dans sa version la plus générale.

Théorème 3.2.1 (Relation A-vs-NA quantique)**.** *Soit $\rho_{\mathsf{AA'B}}$ un état quantique triparti, soit $\mathcal{J}$ un ensemble fini non vide et soit $\mathbf{E} = \{E^j\}_{j\in\mathcal{J}}$ une famille de mesures POVM à résultat binaire E^j qui agissent sur le registre B. Alors,*

$$P_{\mathrm{succ}}(\rho_{\mathsf{AA'B}}, \mathbf{E}) \leq 2^{\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho} P_{\mathrm{succ}}(\rho_{\mathsf{A'B}}, \mathbf{E}) \ .$$

Démonstration. Soit $\{F_j\}_{j\in\mathcal{J}}$ une mesure POVM sur $\mathsf{AA'}$ et soit $\mathcal{M}_{\mathsf{AA'}\to\mathsf{J}}$ l'opération quantique correspondant à cette mesure : $\mathcal{M}(\sigma_{\mathsf{AA'}}) := \sum_j \mathrm{tr}(F_j\sigma_{\mathsf{AA'}})|j\rangle\langle j|_J$. Définissons le super-opérateur suivant

$$\mathcal{E}_{\mathsf{JB}\to\mathbb{C}}(\sigma_{\mathsf{JB}}) := \sum_j \mathrm{tr}\left((|j\rangle\langle j|_{\mathsf{J}} \otimes E_1^j)\sigma_{\mathsf{JB}}\right) \ .$$

Celui-ci est complètement positif et n'augmente pas la trace (c'est un CPTN tel que défini à la section 2.3). Par la définition de la max-information accessible, on sait qu'il existe une mesure $\mathcal{N}_{\mathsf{A'}\to\mathsf{J}}$, de la forme $\mathcal{N}(\sigma_{\mathsf{A'}}) = \sum_j \mathrm{tr}(F'_j\sigma_{\mathsf{A'}})|j\rangle\langle j|_{\mathsf{J}}$ pour un certain POVM $\{F'_j\}_{j\in\mathcal{J}}$ qui agit sur $\mathsf{A'}$, telle que

$$\mathcal{M}_{\mathsf{AA'}}(\rho_{\mathsf{AA'B}}) \leq 2^{\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho}\mathcal{N}_{\mathsf{A'}}(\rho_{\mathsf{A'B}}) \ .$$

En appliquant le super-opérateur $\mathcal{E}_{\mathsf{JB}\to\mathbb{C}}$ des deux côtés de cette dernière inégalité, on obtient

$$(\mathcal{E}_{\mathsf{JB}} \circ (\mathcal{M}_{\mathsf{AA'}} \otimes \mathrm{id}_{\mathsf{B}}))(\rho_{\mathsf{AA'B}}) \leq 2^{\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho}(\mathcal{E}_{\mathsf{JB}} \circ (\mathcal{N}_{\mathsf{A'}} \otimes \mathrm{id}_{\mathsf{B}}))(\rho_{\mathsf{A'B}}) \ .$$

En écrivant au long les définitions de $\mathcal{E}$, $\mathcal{M}$ et $\mathcal{N}$ on trouve

$$\begin{aligned}\sum_j \mathrm{tr}\left((F_j \otimes E_1^j)\rho_{\mathsf{AA'B}}\right) &\leq 2^{\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho}\sum_j \mathrm{tr}\left((F'_j \otimes E_1^j)\rho_{\mathsf{A'B}}\right) \\ &\leq 2^{\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho} P_{\mathrm{succ}}(\rho_{\mathsf{A'B}}, \mathbf{E}) \ .\end{aligned}$$

Ceci complète la preuve de l'énoncé, car en maximisant la partie de gauche de l'inégalité ci-dessus sur tous les POVM $\{F_j\}_{j\in\mathcal{J}}$, on retrouve la définition de $P_{\mathrm{succ}}(\rho_{\mathsf{AA'B}}, \mathbf{E})$. □

En considérant un registre A' trivial, on obtient immédiatement le Corollaire suivant.

Corollaire 3.2.1. *Soit ρ_{AB} un état quantique biparti, soit $\mathcal{J}$ un ensemble fini non vide et soit $\mathbf{E} = \{E^j\}_{j\in\mathcal{J}}$ une famille de mesures POVM à résultat binaire E^j qui agissent sur le registre B. Alors,*

$$P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^{\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_\rho} P^{\mathrm{NA}}_{\mathrm{succ}} \ .$$

Par la Propriété 3.2.1 de la sous-section suivante, on voit que le Corollaire 3.2.1 implique une généralisation de la relation A-vs-NA classique pour les adversaires quantiques. Autrement dit, si l'adversaire dispose de n qubits d'information auxiliaire, alors

$$P^{\mathrm{A}}_{\mathrm{succ}} \leq 2^n P^{\mathrm{NA}}_{\mathrm{succ}}$$

pour $P^{\mathrm{A}}_{\mathrm{succ}}$ et $P^{\mathrm{NA}}_{\mathrm{succ}}$ tels que définis dans la définition 3.2.1.

3.2.1 Propriétés de la max-information accessible

Cette section énonce quelques propriétés de la max-information accessible.

Propriété 3.2.1. *Pour tout ρ_{AB}, on a que $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_\rho \leq \mathrm{H}_0(\mathsf{A})_\rho$.*

Démonstration. Soit $|\rho_{\mathsf{ABR}}\rangle$ une purification de ρ_{AB} et soit $\mathcal{M}_{\mathsf{A}\to\mathsf{X}}$ une mesure sur le registre A. Puisque $|\rho_{\mathsf{ABR}}\rangle$ est aussi une purification de ρ_{A}, il existe un opérateur linéaire $V_{\bar{\mathsf{A}}\to\mathsf{BR}}$ (qui agit sur un registre $\bar{\mathsf{A}}$ de même dimension que A et qui produit les registres BR) tel que $|\rho_{\mathsf{ABR}}\rangle = (\mathbb{1}_{\mathsf{A}} \otimes V_{\bar{\mathsf{A}}})|\Phi_{\mathsf{A}\bar{\mathsf{A}}}\rangle$, où $|\Phi_{\mathsf{A}\bar{\mathsf{A}}}\rangle = \sum_i |i\rangle_{\mathsf{A}} \otimes |i\rangle_{\bar{\mathsf{A}}}$ est un vecteur non normalisé. Remarquons d'abord que

$$2^{-\mathrm{H}_0(\mathsf{A})_\rho}(\mathcal{M}_{\mathsf{A}} \otimes \mathrm{id}_{\bar{\mathsf{A}}})(\Phi_{\mathsf{A}\bar{\mathsf{A}}}) = \sum_x \lambda_x |x\rangle\langle x|_{\mathsf{X}} \otimes \omega^x_{\bar{\mathsf{A}}} \leq \sum_x \lambda_x |x\rangle\langle x|_{\mathsf{X}} \otimes \mathbb{1}_{\bar{\mathsf{A}}} \ , \tag{3.8}$$

où $\{\lambda_x\}$ est la distribution de probabilité correspondant au résultat de la mesure $\mathcal{M}$, et où $\omega^x_{\bar{\mathsf{A}}}$, l'état de $\bar{\mathsf{A}}$ conditionné sur le résultat x, est normalisé, car $\mathrm{tr}(\Phi_{\mathsf{A}\bar{\mathsf{A}}}) = 2^{\mathrm{H}_0(\mathsf{A})_\rho}$. En multipliant chaque côté de l'inégalité (3.8) par $2^{\mathrm{H}_0(\mathsf{A})_\rho}$ et en conjuguant par $V_{\bar{\mathsf{A}}\to\mathsf{BR}}$, on obtient

$$(\mathcal{M}_{\mathsf{A}} \otimes \mathrm{id}_{\mathsf{BR}})(|\rho\rangle\langle\rho|_{\mathsf{ABR}}) \leq 2^{\mathrm{H}_0(\mathsf{A})_\rho} \sum_x \lambda_x |x\rangle\langle x|_{\mathsf{X}} \otimes VV^* \ .$$

En observant que $VV^* = \rho_{\mathsf{BR}} := \mathrm{tr}_{\mathsf{A}}(|\rho\rangle\langle\rho|_{\mathsf{ABR}})$, l'inégalité ci-dessus devient, lorsqu'on prend la trace partielle sur le registre R de chaque côté,

$$(\mathcal{M}_{\mathsf{A}} \otimes \mathrm{id}_{\mathsf{B}})(\rho_{\mathsf{AB}}) \leq 2^{\mathrm{H}_0(\mathsf{A})_\rho} \sigma_{\mathsf{X}} \otimes \rho_{\mathsf{B}} \ ,$$

où $\sigma_{\mathsf{X}} = \sum_x \lambda_x |x\rangle\langle x|_{\mathsf{X}}$. Ceci complète la preuve en observant que l'inégalité ci-dessus correspond à l'inégalité (3.7) de la définition 3.2.2, ce qui implique que $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_\rho \leq \mathrm{H}_0(\mathsf{A})_\rho$. □

On pourrait être tenté de croire que la version conditionnelle de la max-information accessible satisfait également la borne supérieure démontrée ci-dessus, c'est-à-dire que $\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho$ est borné supérieurement par $\mathrm{H}_0(\mathsf{A})_\rho$. Ceci impliquerait un énoncé correspondant pour les adversaires *semi-adaptés* : donner accès à n qubits *additionnels* ne peut augmenter la probabilité de succès que par un facteur de 2^n. Toutefois, ce n'est pas le cas ; une borne semblable ne tient pas pour $\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{A}')_\rho$ comme le démontre le contre-exemple suivant. Considérons les registres quantiques A et A' et le registre B (qui est classique dans cet exemple). L'état de ces registres est le suivant : B contient deux bits classiques aléatoires et les registres A et A' contiennent un des quatre états de Bell, lequel est spécifié par les deux bits de B. Par exemple, l'état $\rho_{\mathsf{AA}'\mathsf{B}}$ peut être décrit par l'état pur

$$\frac{1}{4}\left(\left|\Phi^+\right\rangle_{\mathsf{AA}'}|00\rangle_B + \left|\Phi^-\right\rangle_{\mathsf{AA}'}|01\rangle_B + \left|\Psi^+\right\rangle_{\mathsf{AA}'}|10\rangle_B + \left|\Psi^-\right\rangle_{\mathsf{AA}'}|11\rangle_B\right)$$

où $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle$ et $|\Psi^-\rangle$ sont les quatre états de la base de Bell. Le but d'Alice est de deviner la valeur des deux bits classiques de B. Clairement, Alice peut réussir avec certitude avec la stratégie adaptée qui consiste à mesurer AA' dans la base de Bell. Toutefois, le registre A' à lui seul est inutile pour déterminer la valeur de B car l'état réduit de A' est $\frac{1}{2}\mathbb{1}_{\mathsf{A}'}$ pour n'importe quel état de Bell. Ainsi, la probabilité de succès de la stratégie adaptée est 4 fois supérieure à la probabilité semi-adaptée avec seulement 1 qubit de plus.

Toutefois, la Propriété ci-dessus se généralise à la version conditionnelle pour le cas spécial où A' est classique, tel que montré par la Propriété suivante. Ainsi, lorsqu'un adversaire dispose d'information auxiliaire classique en plus de son registre quantique, on peut généralement l'ignorer lorsqu'on analyse l'information auxiliaire quantique.

Propriété 3.2.2. *Soit* $\rho_{\mathsf{ZAB}} = \sum_z P_Z(z)|z\rangle\langle z|_{\mathsf{Z}} \otimes \rho_{\mathsf{AB}}^z$ *un état classique-quantique-quantique, alors*

$$\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{Z})_\rho \leq \max_z \mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A})_{\rho^z} \leq \mathrm{H}_\infty(\mathsf{A})_\rho \ .$$

Démonstration. Soit $\mathcal{M}_{\mathsf{ZA}\to\mathsf{X}}$ une mesure sur les registres Z et A. Par linéarité, et par la définition de $\mathrm{I}_{\max}^{\mathrm{acc}}$, on a que

$$\begin{aligned}(\mathcal{M}_{\mathsf{ZA}} \otimes \mathrm{id}_{\mathsf{B}})(\rho_{\mathsf{ZAB}}) &= \sum_z P_Z(z)(\mathcal{M}_{\mathsf{ZA}} \otimes \mathrm{id}_{\mathsf{B}})\left(|z\rangle\langle z|_{\mathsf{Z}} \otimes \rho_{\mathsf{AB}}^z\right) \\ &\leq \sum_z P_Z(z) \cdot 2^{\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{Z})_{|z\rangle\langle z|\otimes\rho^z}} (\mathcal{N}_{\mathsf{Z}}^z \otimes \mathrm{id}_{\mathsf{B}})\left(|z\rangle\langle z|_{\mathsf{Z}} \otimes \rho_{\mathsf{B}}^z\right)\end{aligned}$$

pour un choix approprié de mesures $\mathcal{N}_{\mathsf{Z}\to\mathsf{X}}^z$. Si on remarque maintenant que $\mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A}|\mathsf{Z})_{|z\rangle\langle z|\otimes\rho^z} = \mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A})_{\rho^z}$, et qu'il existe une mesure fixe $\mathcal{N}_{\mathsf{Z}\to\mathsf{X}}$ telle que $\mathcal{N}_{\mathsf{Z}}^z(|z\rangle\langle z|) = \mathcal{N}_{\mathsf{Z}}(|z\rangle\langle z|)$ pour tout z, il s'en suit que

$$(\mathcal{M}_{\mathsf{ZA}} \otimes \mathrm{id}_{\mathsf{B}})(\rho_{\mathsf{ZAB}}) \leq 2^{\max_z \mathrm{I}_{\max}^{\mathrm{acc}}(\mathsf{B};\mathsf{A})_{\rho^z}} (\mathcal{N}_{\mathsf{Z}} \otimes \mathrm{id}_{\mathsf{B}})(\rho_{\mathsf{ZB}}) \ .$$

Ceci démontre la première inégalité de l'énoncé. La seconde inégalité découle directement du fait que $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho^z} \leq \mathrm{H}_0(\mathsf{A})_{\rho^z} \leq \mathrm{H}_0(\mathsf{A})_{\rho}$. □

Une autre propriété souhaitable de la max-information accessible est qu'elle ne puisse pas augmenter sous des opérations quantiques séparées (de la forme $\mathcal{E}_{\mathsf{A}} \otimes \mathcal{E}_{\mathsf{B}}$) sur les registres A et B.

Propriété 3.2.3. *Soit $\mathcal{E}_{\mathsf{AB}\to\mathsf{A'B'}}$ un CPTP de la forme $\mathcal{E} = \mathcal{E}_{\mathsf{A}\to\mathsf{A'}} \otimes \mathcal{E}_{\mathsf{B}\to\mathsf{B'}}$. Alors*

$$\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B'};\mathsf{A'})_{\mathcal{E}(\rho)} \leq \mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho} \ .$$

Démonstration. Il est clair que le CPTP $\mathcal{E}_{\mathsf{B}}$ ne peut pas augmenter $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho}$ puisqu'il commute avec toute mesure sur le registre A.

Pour montrer que $\mathcal{E}_{\mathsf{A}}$ ne peut pas non plus augmenter $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho}$, il suffit de remarquer que le super-opérateur $\mathcal{M}_{\mathsf{A}} \circ \mathcal{E}_{\mathsf{A}}$ est aussi une mesure. Donc, par la définition 3.2.2,

$$(\mathcal{M}_{\mathsf{A}} \circ \mathcal{E}_{\mathsf{A}})(\rho_{\mathsf{AB}}) \leq 2^{\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho}} \sigma_{\mathsf{X}} \otimes \rho_{\mathsf{B}}$$

ce qui prouve l'énoncé. □

3.3 Complétude de la primitive 1CC

Dans cette section, nous voyons un premier cas où notre réduction des stratégies adaptées aux non adaptées a permis de résoudre un problème ouvert où une analyse directe aurait été difficile. En utilisant notre relation A-vs-NA, il suffit de borner la max-information accessible et d'analyser le comportement d'un adversaire non adapté, ce qui facilite grandement la tâche.

Nous montrons que la primitive 1CC est universelle dans le modèle UC, résolvant ainsi la principale question ouverte de [FKS+13]. Pour ce faire, nous construisons un protocole de mise en gage quantique qui utilise l'accès à une fonctionnalité idéale $\mathcal{F}_{\text{1CC}}$ comme hypothèse. Nous montrons d'abord la sécurité de ce protocole de mise en gage dans le modèle à sécurité autonome dans la sous-section 3.3.2, ce qui permet de mettre la table pour la preuve complète que 1CC est complète dans le modèle UC dans la sous-section 3.3.3.

3.3.1 Le protocole de mise en gage

Le protocole de mise en gage faisant l'objet de cette section est décrit dans la figure 3.2. Dans ce protocole, Alice est celle qui se met en gage et Bob est le receveur de la mise en gage. Le protocole est

Participants : L'envoyeuse Alice et le receveur Bob.

Entrées : Alice reçoit $b \in \{0,1\}$ et Bob ne reçoit aucune entrée.

$\textsc{mise-en-gage}^{1\text{CC}}_{N,q,\tau,r}(b)$:

1. Alice choisit une base aléatoire $\theta \in \{0,1\}^N$ selon la distribution uniforme et envoie N qubits dans l'état $H^{\otimes\theta}|0^N\rangle$ à Bob où H est la transformée de Hadamard.
2. Pour $i = 1 \dots N$, Alice et Bob font un appel à $\mathcal{F}_{1\text{CC}}$: Alice entre le bit θ_i, Bob entre le bit 1 avec probabilité q et le bit 0 avec probabilité $1-q$.

   Soit $t \subset [N]$ l'ensemble des positions pour lesquelles l'entrée de Bob est 1, soit $\bar{t} = [N] \setminus t$, et soit $n = N - |t|$. Alice interrompt le protocole si Bob a vérifié plus de $2qN$ positions.
3. Pour tout $i \in t$, Bob mesure le i^{e} qubit du registre qu'il a reçu d'Alice dans la base θ_i et vérifie que le résultat est $H^{\theta_i}|0\rangle$. Si ce n'est pas le cas, il interrompt le protocole.
4. Bob choisit une matrice génératrice G d'un $[n,k,d]$-code correcteur linéaire avec taux $k/n \geq r$ et $d/n \geq \tau$, et il envoie G à Alice, qui vérifie que $k/n \geq r$.
5. Alice choisit aléatoirement une fonction $g \in_R \mathcal{G}_n$ parmi une famille $\mathcal{G}_n$ de fonctions de hachage deux-universelles. Elle calcule le syndrome s de $\theta_{\bar{t}}$ pour le code correcteur. Finalement, elle envoie g, s et $w = g(\theta_{\bar{t}}) \oplus b$ à Bob. À la réception de ces informations, Bob produit la sortie `mise-en-gage`.

$\textsc{ouverture}^{1\text{CC}}$:

1. Alice envoie $\theta_{\bar{t}}$ et b à Bob.
2. Bob mesure le i^{e} qubit dans la base θ_i pour chaque $i \in \bar{t}$ et vérifie que le résultat correspond à $H^{\theta_i}|0\rangle$. Il s'assure aussi que $\theta_{\bar{t}}$ a syndrome s pour le code correcteur généré par G, et que $g(\theta_{\bar{t}}) \oplus w = b$. Si un des tests ci-dessus échoue, il avorte le protocole. Sinon, il produit la sortie b.

FIGURE 3.2 – Protocole de mise en gage $\Pi^{\mathcal{F}_{1\text{CC}}}_{\text{BC}}$ utilisant la primitive transfert sélectif à un bit. Pour se mettre en gage à $b \in \{0,1\}$, Alice et Bob exécutent le sous-protocole $\textsc{mise-en-gage}^{1\text{CC}}_{N,q,\tau,r}(b)$ avec les paramètres appropriés. Pour ouvrir la mise en gage, ils exécutent le sous-protocole $\textsc{ouverture}^{1\text{CC}}$.

paramétré par $N \in \mathbb{N}$, qui sert de paramètre de sécurité, et par les valeurs réelles q, τ et r où $q, \tau > 0$ sont près de 0 et $r < 1$ près de 1.

Notre protocole utilise essentiellement des outils standards ; l'utilisation d'un code correcteur pour que le protocole soit contraignant et de l'amplification de l'incertitude pour qu'il soit camouflant. Là où notre protocole diffère des constructions habituelles est par l'utilisation de l'encodage B92 [Ben92] (composé des deux états $\{|0\rangle, |+\rangle\}$), plutôt que l'encodage BB84 [BB84] à quatre états qui est plus commun — et qui serait le choix naturel et plus efficace pour ce type de protocole. Cette particularité est due au fait que nous utilisons la primitive 1CC, une primitive à *un* bit, et ainsi la description de l'état transmis doit tenir dans un bit. Avec un encodage BB84, il aurait fallu une primitive avec *deux* bits d'entrée du côté d'Alice : un pour la base et un autre pour le résultat de mesure. Notons que c'est l'approche prise dans [FKS+13] : ils échantillonnent des états BB84 en utilisant la fonctionnalité 2CC.

Intuitivement, notre protocole de mise en gage utilise la primitive 1CC pour s'assurer que l'état qu'Alice envoie à Bob pendant la phase de mise en gage est près de l'état qu'elle doit envoyer. La primitive 1CC permet en effet à Bob de vérifier — ou *d'échantillonner* — les qubits envoyés par Alice : celle-ci entre dans le 1CC la description de l'état envoyé à Bob et celui-ci mesure l'état reçu en fonction de cette description. Si aucune erreur n'est observée, c'est-à-dire si chaque résultat de mesure est en accord avec la description fournie par Alice, on peut s'attendre à ce que l'état des qubits non observés ne soit pas trop loin de l'état honnête. Les primitives du type transfert sélectif se prêtent en effet bien à ce genre d'exercice ; Alice entre une certaine information dans la boîte $\mathcal{F}_{m\text{CC}}$ (dans notre cas, la description de l'état) et Bob entre un bit qui indique s'il souhaite échantillonner ou non cette position. La primitive fait en sorte que l'information qu'Alice entre dans la boîte i est indépendante du choix de Bob d'échantillonner la position i et qu'à la fin de l'échantillonnage Alice connaît les positions qui ont été vues par Bob.

La preuve de sécurité du protocole de mise en gage $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$ utilise la procédure d'échantillonnage quantique de Bouman et Fehr [BF10] afin d'analyser la procédure de vérification décrite plus haut, qui correspond à l'étape 2 de la phase de mise en gage. Plus précisément, nous utilisons la version *adaptative* de leur procédure d'échantillonnage [FKS+13], ce qui permet de gérer le cas où Alice peut décider de la base à annoncer en fonction des positions que Bob a demandées de voir jusqu'à présent, autrement dit, θ_i peut dépendre de $\theta_1, \ldots, \theta_{i-1}$ et de $t_1, \ldots, t_{i-1}$. De l'autre côté, pour contrôler les attaques possibles du côté de Bob, on ne lui permet de choisir que des échantillons de petite taille (une fraction q constante, mais petite, du nombre de positions N). Cette restriction fait en sorte que s'il tente de choisir les positions de θ qu'il veut voir en fonction de ce qu'il a vu jusqu'à présent ou encore en fonction d'une mesure sur sa partie de l'état conjoint, la petite taille de l'échantillon suffira à limiter sa probabilité de deviner le bit mis en gage. Pour cette raison, Alice avorte le protocole si Bob demande de voir trop de positions, soit plus de $2qN$ position ; une éventualité qui n'arrive qu'avec probabilité négligeable si Bob est honnête (par

le théorème de Hoeffding).

3.3.2 Sûreté du protocole de mise en gage dans le modèle à sécurité autonome

Dans cette section, nous montrons la sûreté de notre protocole de mise en gage (figure 3.2) selon la définition standard de sécurité pour cette tâche cryptographique. Cette définition comprend deux parties, une pour chaque participant, soit le fait d'être camouflant (définition 3.3.1) et le fait d'être contraignant (définition 3.3.2). Cette preuve de sécurité en soi n'est pas suffisante pour démontrer le résultat principal de cette section, c'est-à-dire que la primitive 1CC est universelle de manière universellement composable, mais elle donne toutefois l'intuition derrière la sécurité et servira de base pour montrer la sécurité dans le modèle UC.

Le protocole est camouflant

Nous utilisons la définition usuelle pour la notion de camouflage du bit mis en gage. Cette définition est la suivante, elle dit que du point de vue du receveur, le bit auquel l'envoyeur s'est mis en gage est indistinguable d'un bit aléatoire.

Définition 3.3.1 (Camouflant)**.** Un protocole de mise en gage est ϵ-*camouflant* si, pour n'importe quelle stratégie du receveur Bob, l'état ρ_0 de son registre correspondant à une mise en gage de $b = 0$ et l'état ρ_1 correspondant de $b = 1$ satisfont $D(\rho_0, \rho_1) \leq \epsilon$.

La preuve que notre protocole de mise en gage satisfait la définition 3.3.1 utilise une approche standard, il s'agit de montrer que la chaine $\theta_{\bar{t}}$, qui sert à camoufler le bit mis en gage, a suffisamment de min-entropie du point de vue de Bob. L'amplification de l'incertitude (étape 5 du protocole) complète alors la preuve en convertissant cette incertitude sur $\theta_{\bar{t}}$ en incertitude sur le bit mis en gage.

Théorème 3.3.1. *Le protocole* $\Pi_{\mathrm{BC}}^{\mathcal{F}_{1\mathrm{CC}}}$ *est* $2^{-\frac{1}{2}N(\lg(1/\gamma)-2q-(1-r)-3)}$*-camouflant, où* $\gamma = \cos^2(\pi/8) \approx 0.85$ *(et donc* $\lg(1/\gamma) \approx 0.23$*).*

Démonstration. Pour montrer que le bit b est bien camouflé par $g(\theta_{\bar{t}})$, il faut montrer que pour tout choix de $t \subset [N]$, Bob a suffisamment d'incertitude sur la valeur exacte de $\theta_{\bar{t}}$, calculée en termes de min-entropie [4], pour pouvoir appliquer l'amplification d'incertitude. Ceci équivaut à montrer que la probabilité que Bob devine la valeur exacte de $\theta_{\bar{t}}$ est négligeable en N. Ce qui rend l'argument légèrement non trivial

4. Pour être entièrement formel, il faudrait considérer une variable aléatoire Θ représentant les valeurs possibles de θ avec les probabilités associées.

est que Bob peut choisir l'échantillon t en fonction de l'état $H^{\otimes\theta}|0^N\rangle$ qu'il détient et des positions de θ qu'il a vu jusqu'à présent par l'entremise des appels à 1CC. Par contre, puisqu'Alice avorte le protocole si $|t| > 2qN$, on suppose pour la preuve que $|t| \leq 2qN$.

La probabilité que Bob devine la valeur de $\theta \in \{0,1\}^N$ tout juste après l'étape 1 du protocole, c'est-à-dire s'il dispose seulement de l'état $H^{\otimes\theta}|0^N\rangle$ comme information sur θ, est donnée par la probabilité maximale de distinguer les 2^N états possibles de cette forme. Puisque chacune des positions de θ est choisie de manière indépendante et uniforme, cette probabilité est égale à γ^N où, par le théorème de Helström,

$$\gamma := \frac{1}{2} + \frac{1}{4}\,\big\||0\rangle\langle 0| - |+\rangle\langle +|\big\|_1 = \cos^2(\pi/8) \approx 0.85$$

est la probabilité maximale de distinguer les états $|0\rangle$ et $|+\rangle$ lorsqu'ils sont équiprobables. À partir de cette observation, on peut déduire que sa probabilité de deviner $\theta_{\bar{t}}$ après l'étape 2 est au plus $\gamma^N \cdot 2^{2qN}$ peut importe la valeur de t, en vertu de la version classique de la relation A-vs-NA. En effet, si cette probabilité était plus grande, alors Bob pourrait deviner θ avec probabilité meilleure que γ^N après l'étape 1 en simulant l'interaction avec Alice qui a lieu à l'étape 2 et en *devinant* les $|t| \leq 2qN$ valeurs θ_i qu'Alice lui fournit durant cette interaction, ce qui mène à une contradiction. Il en découle qu'après l'étape 2, la min-entropie de $\theta_{\bar{t}}$ du point de vue de Bob est d'au moins $N(\lg(1/\gamma) - 2q)$.

La seule information supplémentaire que Bob apprend sur $\theta_{\bar{t}}$ est son syndrome s pour le code correcteur. Ce syndrome fournit à Bob au plus $n-k$ bits d'information sur $\theta_{\bar{t}}$, soit la taille de s. En utilisant la règle de chaine pour la min-entropie, la min-entropie de $\theta_{\bar{t}}$ à la fin du protocole de mise en gage est au moins

$$N\big(\lg(1/\gamma) - 2q\big) - (n-k) = N\big(\lg(1/\gamma) - 2q\big) - n(1-k/n) \geq N\big(\lg(1/\gamma) - 2q - (1-r)\big)\ .$$

Par le théorème d'amplification de l'incertitude (théorème 2.6.1), on a alors que

$$D(\rho_{\mathsf{WB}}, \frac{\mathbb{1}}{2} \otimes \rho_{\mathsf{B}}) \leq 2^{-\frac{1}{2}(N(\lg(1/\gamma)-2q-(1-r))-1)} \tag{3.9}$$

où le registre classique W contient la valeur $w = g(\theta_{\bar{t}})$ envoyée à Bob à la fin de la mise en gage et où on suppose que le registre quantique B contient toutes les informations connues par Bob. Puisqu'on cherche à borner la distance de trace entre les états ρ^0 et ρ^1 correspondant respectivement à des mises en gage à 0 et à 1, on utilise l'inégalité du triangle sur l'inégalité (3.9) pour montrer que ces états sont indistinguables :

$$D(\rho^0_{\mathsf{B}}, \rho^1_{\mathsf{B}}) \leq 2 \cdot 2^{-\frac{1}{2}(N(\lg(1/\gamma)-2q-(1-r))-1)}\ .$$

Ceci complète la preuve que le protocole est ϵ-camouflant pour $\epsilon = 2^{-\frac{1}{2}(N(\lg(1/\gamma)-2q-(1-r))-3)}$. □

Le protocole est contraignant

Pour ce qui est de la propriété contraignante de notre protocole de mise en gage, nous arrivons à prouver une définition de sécurité plutôt forte : non seulement on peut garantir l'existence d'un bit b auquel Alice est contrainte, c'est-à-dire tel qu'elle ne peut dévoiler le bit complémentaire $1-b$, mais on peut en plus montrer que ce bit peut être calculé à partir de l'information classique détenue par Bob et des entrées d'Alice dans les boîtes 1CC. Nous nommons cette notion de sécurité *l'extractibilité universelle* [CLOS02], celle-ci dit essentiellement que le bit auquel Alice est liée peut être extrait par un simulateur dans le contexte du modèle UC.

Définition 3.3.2 (Extractibilité Universelle)**.** Un protocole de mise en gage (dans le modèle $\mathcal{F}_{1\text{CC}}$-hybride) est ϵ-*universellement extractible* s'il existe une fonction booléenne $c : \{0,1\}^* \to \{0,1\}$ qui prend comme paramètre l'information classique $X_{Bob,1\text{CC}}$ qu'Alice envoie à Bob et aux boîtes 1CC pendant la phase de mise en gage et qui est telle que pour n'importe quelle stratégie d'ouverture d'Alice, elle a probabilité au plus ϵ de dévoiler le bit $1 - c(X_{Bob,1\text{CC}})$.

La stratégie pour montrer que le protocole de mise en gage $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$ satisfait la définition 3.3.2 est la suivante. En première partie, nous montrons que l'état conjoint après la phase de vérification par Bob (l'étape 2) est d'une certaine forme avec très forte probabilité. Ensuite, nous montrons que si l'état conjoint a cette forme, alors une stratégie non adaptée (où Alice n'utilise pas sa partie de l'état) aura probabilité négligeable d'ouvrir le « mauvais » bit $1 - c(X_{Bob,1\text{CC}})$. Nous appliquons la relation A-vs-NA quantique pour montrer qu'une stratégie générale (adaptée) ne peut réussir à ouvrir le bit $1 - c(X_{Bob,1\text{CC}})$ avec probabilité meilleure que négligeable.

Le lemme suivant découle directement de (la version adaptative de) l'échantillonnage quantique de Bouman et Fehr [BF10, FKS+13]. Il s'agit d'une forme compressée de leurs résultats avec les paramètres adéquats à notre contexte. Intuitivement, l'échantillonnage quantique peut montrer que si Bob n'a pas avorté le protocole durant l'étape 2 de MISE-EN-GAGE$^{1\text{CC}}_{N,q,\tau,r}(b)$, alors le registre quantique de Bob se trouve dans un état qui est près de l'état correcte (qu'une Alice honnête aurait envoyé) à quelques erreurs près. Autrement dit, sauf avec probabilité négligeable, l'état de Bob après l'étape 2 appartient au sous-espace engendré par les états près (en distance de hamming) de 0^N dans la base spécifiée par $\theta_{\bar{t}}$.

Lemme 3.3.1 (Échantillonnage adaptatif d'états purs [BF10, FKS+13])**.** *Soit ρ_{AB} l'état quantique d'Alice et Bob au début du protocole $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$ et soit*

$$\rho_{\mathsf{T\Theta AB}} = \sum_{\substack{t\subset[N]\\ \theta\in\{0,1\}^N}} P_{T,\Theta}(t,\theta)|t,\theta\rangle\langle t,\theta| \otimes \rho_{\mathsf{AB}}^{t,\theta}$$

l'état juste avant l'étape 3 du protocole incluant les échanges classiques par les boîtes 1CC *et les dépendances*

que l'état de Bob puisse avoir sur ces échanges. Il existe une famille d'états $\tilde{\rho}^{t,\theta}_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ *telle que*

$$D\left(\rho_{\mathsf{T\Theta AB}}\ ,\ \sum_{t,\theta} P_{T,\Theta}(t,\theta)|t,\theta\rangle\langle t,\theta| \otimes \tilde{\rho}^{t,\theta}_{\mathsf{AB}}\right) \leq 2\exp(-q^2\delta^2 N/16)$$

où $\mathrm{supp}(\tilde{\rho}^{t,\theta}_{\mathsf{AB}}) \subseteq \mathcal{H}_{\mathsf{A}} \otimes \mathrm{span}\{H^{\otimes\theta}|x\rangle\ :\ |w(x_t) - w(x_{\bar{t}})| \leq \delta\}$ *pour tout* t, θ.

La leçon à tirer du lemme précédent est que si l'état d'Alice et Bob tout juste avant l'étape 3 du protocole de mise en gage est $\tilde{\rho}^{t,\theta}_{\mathsf{AB}}$ (conditionné sur l'échantillon t et les valeurs θ entrées dans les 1CC), et si Bob observe l'état $H^{\otimes\theta_t}|0^{|t|}\rangle$ pour les positions mesurées, alors l'état résiduel des n qubits de Bob conditionné sur ce résultat est, *avec certitude*, dans un sous-espace engendré par les états de la forme $H^{\theta_{\bar{t}}}|x\rangle$ pour $x \in \{0,1\}^n$ tel que $w(x) \leq \delta$.

Le lemme suivant montre que si l'état conjoint a la forme décrite ci-dessus et que Bob accepte l'issue de l'échantillonnage, alors Alice a probabilité négligeable d'ouvrir le bit $1 - c(X_{Bob,1\mathrm{CC}})$. L'intuition derrière celui-ci est que si l'état de Bob est *bien défini* dans une certaine base $\hat{\theta}$, c'est-à-dire tel qu'il y a peu d'incertitude sur le résultat de mesure dans cette base, alors pour tout syndrome s, il y a au plus une seule base qu'Alice peut annoncer pendant la phase d'ouverture et qui sera acceptée avec probabilité non négligeable par Bob. Le lemme établit l'existence pour tout s d'une base θ' de syndrome s telle que pour toute autre base θ'' de même syndrome, le résultat de mesure dans la base θ'' aura beaucoup d'incertitude.

Lemme 3.3.2. *Soit* $\hat{\theta} \in \{0,1\}^n$, $s \in \{0,1\}^{n-k}$ *et soit* $\tilde{\rho}_{\mathsf{B}}$ *qui a support dans* $\mathrm{span}\{H^{\otimes\hat{\theta}}|x\rangle\ :\ w(x) \leq \delta\}$. *Il existe* $\theta' \in \{0,1\}^n$ *avec syndrome* s *tel que pour tout* $\theta'' \neq \theta'$ *avec syndrome* s,

$$\mathrm{tr}\left(H^{\otimes\theta''}|0\rangle\langle 0|H^{\otimes\theta''}\tilde{\rho}_{\mathsf{B}}\right) \leq 2^{-\frac{d}{2}+nh(\delta)}\ . \tag{3.10}$$

Démonstration. Soit $\theta' \in \{0,1\}^n$ la chaine de bit avec syndrome s la plus près de $\hat{\theta}$ (en distance de hamming). Alors, puisque l'ensemble des chaines avec un même syndrome forme un code correcteur de distance d, chacune des autres chaines $\theta'' \in \{0,1\}^n$ de syndrome s est à distance au moins d de θ'. Par l'inégalité du triangle, on peut en déduire que $d(\hat{\theta}, \theta'') \geq d/2$.

Considérons maintenant la partie gauche de (3.10). En utilisant le fait que $\rho \leq \mathbb{1}_{\mathrm{supp}(\rho)}$ pour tout opérateur de densité ρ,

$$\begin{aligned}
\mathrm{tr}\left(H^{\otimes\theta''}|0\rangle\langle 0|H^{\otimes\theta''}\tilde{\rho}_{\mathsf{B}}\right) &\leq \mathrm{tr}\left(H^{\theta''}|0\rangle\langle 0|H^{\theta''}\left(\sum_{x\,:\,w(x)\leq\delta n} H^{\otimes\hat{\theta}}|x\rangle\langle x|H^{\otimes\hat{\theta}}\right)\right) \\
&= \sum_{x\,:\,w(x)\leq\delta n} |\langle x|H^{\otimes\hat{\theta}}H^{\otimes\theta''}|0\rangle|^2 \\
&\leq 2^{-\frac{d}{2}+nh(\delta)}
\end{aligned}$$

où la dernière inégalité découle du fait que chacun des termes de la somme est borné supérieurement par $2^{-\frac{d}{2}}$ (par la distance de Hamming entre $\hat{\theta}$ et θ'') et que la somme contient au plus $2^{nh(\delta)}$ éléments. □

Nous sommes maintenant prêts à prouver que notre protocole de mise en gage satisfait la définition 3.3.2.

Théorème 3.3.2. *Pour tout $\delta > 0$, le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$ est ϵ-universellement extractible pour*

$$\epsilon \leq 2^{-N(1-2q)(\tau/2-2h(\delta))} + 2\exp(-q^2\delta^2 N/16) \ .$$

Démonstration. On doit montrer l'existence d'une fonction binaire c prenant en entrée toutes les informations classiques détenues par Bob et les boîtes 1CC (soit θ, t, g, w et s) et qui satisfait la propriété de la définition 3.3.2, c'est-à-dire telle que pour toute stratégie de mise en gage, il n'y a aucune stratégie d'ouverture qui permette l'ouverture de $1 - c(\theta, t, g, w, s)$, sauf avec probabilité négligeable. Cette fonction est définie comme $c(t, \theta, g, w, s) := g(\theta') \oplus w$ où la base $\theta' \in \{0,1\}^n$ est telle que définie dans le lemme 3.3.2, c'est-à-dire que θ' est la chaine de syndrome s la plus près de $\theta_{\bar{t}}$ (qui dépend donc seulement de θ, t et s).

Considérons maintenant une stratégie arbitraire d'Alice pour le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$. Soit ρ_{AB} l'état préparé par Alice au tout début de la phase de mise en gage où le registre A est gardé par Alice et B est envoyé à Bob. Soient $t \subset [N]$ l'échantillon choisi par Bob et θ la chaine choisie par Alice comme entrée dans les 1CC (qui peut dépendre de t) et soit $\rho_{\mathsf{AB}}^{t,\theta}$ l'état conjoint après l'étape d'échantillonnage du protocole (l'étape 2) conditionné sur ces choix de t et θ. Par le lemme 3.3.1, on sait que pour tout $\delta > 0$, l'état conjoint $\rho_{\mathsf{AB}}^{t,\theta}$ se comporte de manière identique à un état idéal $\tilde{\rho}_{\mathsf{AB}}$ qui a support dans $\mathcal{H}_{\mathsf{A}} \otimes \text{span}\{H^{\otimes\theta}|x\rangle \ : \ |w(x_t) - w(x_{\bar{t}})| \leq \delta n\}$ (où nous laissons la dépendance sur t et θ implicite) sauf avec probabilité $\epsilon_1 \leq 2\exp(-q^2\delta^2 N/16)$ sur les choix de θ et t. Finalement, soient g, w et s les valeurs envoyées à Bob à la fin de la phase de mise en gage, ce qui nous permet maintenant de définir le bit $c := c(t, \theta, g, w, s)$ auquel nous montrerons qu'Alice est contrainte.

Supposons maintenant qu'Alice et Bob partagent l'état idéal $\tilde{\rho}_{\mathsf{AB}}$ et analysons la probabilité qu'Alice puisse tricher, c'est-à-dire ouvrir le bit $1 - c$, à partir de cet état. Nous compenserons ensuite pour le terme ϵ_1 afin de traduire cette probabilité de tricher en celle pour l'état réel. Par le fait que $\tilde{\rho}_{\mathsf{AB}}$ est idéal, l'état conjoint $\tilde{\rho}_{\mathsf{AB}_{\bar{t}}}^{\text{acc}}$ après l'étape 3 du protocole, défini en conditionnant sur le fait que Bob n'ait pas interrompu le protocole (donc qu'il a observé le résultat de mesure 0^k dans la base θ_t), a support dans $\mathcal{H}_{\mathsf{A}} \otimes \text{span}\{H^{\otimes\theta_{\bar{t}}}|x\rangle \ : \ w(x) \leq \delta n\}$. Puisque le reste du protocole consiste en Alice qui envoie les informations classiques g, w et s à Bob (possiblement à partir de mesures faites sur A), l'état de Bob à la fin du protocole $\tilde{\rho}_{\mathsf{B}_{\bar{t}}}^{\text{fin}}$, conditionné sur ces valeurs a toujours support dans le sous-espace $\text{span}\{H^{\otimes\theta_{\bar{t}}}|x\rangle \ : \ w(x) \leq \delta\}$ (car toute opération quantique sur A du côté d'Alice commute avec la projection de $\mathsf{B}_{\bar{t}}$ sur ce sous-espace du côté de Bob).

Soit maintenant $\mathcal{B}$ l'ensemble des chaines $\theta'' \in \{0,1\}^n$ avec syndrome s telles que $g(\theta'') \oplus w = 1 - c$ et soit $\mathbf{E} = \{\{E_0^{\theta''}, E_1^{\theta''}\}\}_{\theta'' \in \mathcal{B}}$ la famille de mesures POVM où $\{E_0^{\theta''}, E_1^{\theta''}\}$ correspond à la mesure que Bob fait pour vérifier l'ouverture de la mise en gage quand Alice annonce θ''. Cette mesure est définie par les opérateurs $E_1^{\theta''} := H^{\otimes\theta''}|0\rangle\langle 0|H^{\otimes\theta''}$ et $E_0^{\theta''} := \mathbb{1} - H^{\otimes\theta''}|0\rangle\langle 0|H^{\otimes\theta''}$. La probabilité maximale qu'Alice réussisse à dévoiler le bit $1-c$ est donc égale à l'expression $P_{\text{succ}}(\tilde{\rho}^{\text{fin}}_{\mathsf{AB}_{\tilde{t}}}, \mathbf{E})$ telle que définie par (3.5) dans la section 3.2. Le reste de la preuve consiste alors à appliquer le corollaire 3.2.1 à cette expression, mais pour ce faire, on doit d'abord contrôler la quantité de max-information accessible dont Alice dispose avec l'état $\rho^{\text{fin}}_{\mathsf{AB}_{\tilde{t}}}$.

Par la propriété 3.2.2, on sait que l'information classique n'aide pas Alice à tricher le protocole, on peut donc se concentrer sur le registre A que détient Alice. Supposons sans perte de généralité que $\tilde{\rho}^{\text{fin}}_{\mathsf{AB}_{\tilde{t}}}$ est pur (car si cet état n'était pas pur, ça ne ferait qu'aider Alice de lui donner le registre de purification). Par le fait que $\text{supp}(\tilde{\rho}^{\text{fin}}_{\mathsf{B}_{\tilde{t}}}) \subseteq \text{span}\{H^{\otimes\theta_{\tilde{t}}}|x\rangle \,:\, w(x) \leq \delta\}$, toute purification de $\tilde{\rho}^{\text{fin}}_{\mathsf{B}_{\tilde{t}}}$ peut s'écrire de la forme

$$\sum_{x\,:\,w(x)\leq\delta} \alpha_x |\xi^x\rangle_{\mathsf{A}} \otimes H^{\otimes\theta_{\tilde{t}}}|x\rangle \tag{3.11}$$

où les $|\xi^x\rangle_{\mathsf{A}}$ sont des états quelconques (pas nécessairement orthogonaux) et où $\sum_x |\alpha_x|^2 = 1$. Puisque le rang de l'état réduit $\tilde{\rho}^{\text{fin}}_{\mathsf{A}}$ du registre A est au plus le nombre de termes dans la somme de (3.11) (nombre qui est borné supérieurement par $2^{nh(\delta)}$), on en conclut que $\text{H}_0(\mathsf{A})_{\tilde{\rho}^{\text{fin}}} = \log(\text{rang}(\tilde{\rho}^{\text{fin}}_{\mathsf{A}})) \leq nh(\delta)$.

On peut maintenant borner la probabilité de tricher d'Alice (d'ouvrir $1-c$) sur l'état idéal $\tilde{\rho}^{\text{fin}}_{\mathsf{AB}_{\tilde{t}}}$:

$$P_{\text{succ}}(\tilde{\rho}^{\text{fin}}_{\mathsf{AB}_{\tilde{t}}}, \mathbf{E}) \leq 2^{\text{H}_0(\mathsf{A})} P_{\text{succ}}(\tilde{\rho}^{\text{fin}}_{\mathsf{B}_{\tilde{t}}}, \mathbf{E}) \leq 2^{-\frac{d}{2}+2nh(\delta)} \leq 2^{-n(\tau/2-2h(\delta))} \tag{3.12}$$

où la première inégalité découle du corollaire 3.2.1 et de la proposition 3.2.1, et la seconde de la borne supérieure sur $\text{H}_0(\mathsf{A})_{\tilde{\rho}^{\text{fin}}}$ et du lemme 3.3.2. En substituant l'état idéal pour l'état réel dans (3.12), on obtient

$$P_{\text{succ}}(\rho^{\text{fin}}_{\mathsf{AB}_{\tilde{t}}}, \mathbf{E}) \leq 2^{-n(\tau/2-2h(\delta))} + 2\exp(-q^2\delta^2 N/16)$$

La preuve est complétée en observant que $n \geq N(1-2q)$. □

Remarque sur le choix du code correcteur

Pour ce qui est du choix des paramètres q, τ et r, et du choix du code correcteur, notons que la borne de Gilbert-Varshamov (théorème 2.7.1 et corollaire 2.7.1) garantit que tant que $r < 1 - h(\tau)$, il existe des codes correcteurs à distance minimale $d \geq \tau n$. Ceci assure la sécurité contre Alice dès que $\tau > 4h(\delta)$. Pour la sécurité contre Bob, nous avons également besoin que la relation $r > 1 - 0.23 + 2q$ soit satisfaite. Ainsi, dès que $h(\tau) < 0.23 - 2q$, il existe un taux r et une matrice génératrice G telle que notre protocole de mise

en gage est sûr contre les deux participants. Comme il est toujours possible de choisir $\delta > 0$ assez petit, il existe un choix de paramètres pour lequel le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ est à la fois contraignant et camouflant.

3.3.3 Complétude de 1CC dans le modèle UC

Nous avons montré que notre protocole de mise en gage $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ implémente $\mathcal{F}_{\text{BC}}$ dans le modèle $\mathcal{F}_{\text{1CC}}$-hybride sous la définition de sécurité autonome. En utilisant la construction standard pour obtenir $\mathcal{F}_{\text{OT}}$ à partir de $\mathcal{F}_{\text{BC}}$ dans le monde quantique [BBCS91, Cré94], on peut conclure que $\mathcal{F}_{\text{OT}} \sqsubseteq \mathcal{F}_{\text{1CC}}$ dans le modèle à sécurité autonome quantique, et puisque $\mathcal{F}_{\text{OT}}$ est universel, on obtient directement l'universalité de $\mathcal{F}_{\text{1CC}}$. Toutefois, nous n'avons pas encore tout à fait résolu le problème ouvert de [FKS+13], la motivation derrière cette section. Le bémol est que [FKS+13] pose le problème de l'universalité de $\mathcal{F}_{\text{1CC}}$ dans le modèle *universellement composable* quantique (voir Section 2.4), c'est-à-dire à savoir si $\mathcal{F}_{\text{1CC}}$ est *UC-complet*. Donc, pour vraiment résoudre le problème ouvert de [FKS+13], il faudrait prouver que la construction standard pour $\mathcal{F}_{\text{OT}}$ qui utilise notre protocole de mise en gage tel que mentionné plus haut est sûr dans le modèle UC, par exemple en argumentant que notre protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ est lui-même sûr dans le modèle UC.

La sûreté de $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ dans le modèle UC contre Alice (envoyeuse) malhonnête découle directement de notre définition du critère contraignant du protocole (définition 3.3.2) ; après la phase de mise en gage, Alice est contrainte à un bit et celui-ci peut être extrait indépendamment d'Alice en regardant seulement l'information classique détenue par Bob et par les boîtes $\mathcal{F}_{\text{1CC}}$. Un simulateur qui réplique intérieurement les interactions entre Alice malhonnête, Bob et les boîtes $\mathcal{F}_{\text{1CC}}$ pourrait donc extraire ce bit et le donner en entrée à la fonctionnalité $\mathcal{F}_{\text{BC}}$ externe (voir la figure 3.4). Puisqu'Alice est contrainte à dévoiler ce bit, cette attaque dans le monde idéal est indistinguable de l'attaque d'Alice dans le monde réel. Il est donc possible de démontrer la sûreté UC de notre protocole contre Alice corrompue ; nous le faisons plus loin dans cette sous-section dans la proposition 3.3.1.

Toutefois, il n'est pas clair que le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ est sûr contre Bob malhonnête dans le modèle UC. Bien que la sécurité contre Bob est la plus facile à prouver dans le modèle autonome, le problème survient lorsqu'on veut montrer que le protocole est *universellement équivocable*. Dans le modèle UC, il n'est pas suffisant de montrer qu'une mise en gage à 0 est indistinguable d'une mise en gage à 1 (définition 3.3.1), il faut montrer qu'un simulateur ayant le contrôle d'Alice et des boîtes $\mathcal{F}_{\text{1CC}}$ peut choisir le bit à dévoiler au moment de l'ouverture. Dans notre cas, il est probablement possible de montrer qu'un tel simulateur existe en purifiant les actions d'Alice et en utilisant l'attaque standard contre les protocoles de mise en gage quantique [May97, LC98], mais il n'est pas évident que cette attaque puisse être réalisée en temps polynomial en celui de l'adversaire. Bien qu'on veuille montrer la sécurité UC *statistique* — et non *calculatoire* — de $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$, la définition de sûreté dans le modèle UC (définition 2.4.2) demande que le

simulateur ait un temps d'exécution polynomial dans le temps d'exécution de l'adversaire.

N'empêche, il est toujours possible d'obtenir un protocole UC-sûr pour $\mathcal{F}_{\text{OT}}$ dans le modèle $\mathcal{F}_{\text{1CC}}$-hybride, et ainsi résoudre le principal problème ouvert de [FKS+13]. Pour ce faire, il faut légèrement modifier le protocole standard pour $\mathcal{F}_{\text{OT}}$ dans le modèle $\mathcal{F}_{\text{BC}}$-hybride [BBCS91, Cré94] avec $\mathcal{F}_{\text{BC}}$ implémenté par $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ comme suit (voir protocole $\Pi_{\text{OT}}^{\mathcal{F}_{\text{1CC}}}$ de la figure 3.7). Pour chaque qubit BB84 que le receveur du protocole doit mesurer, il se met en gage à la base en utilisant le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$, mais utilise la fonctionnalité $\mathcal{F}_{\text{1CC}}$ pour se « commettre » directement au résultat de sa mesure, autrement dit, le receveur entre les résultats de mesure dans les $\mathcal{F}_{\text{1CC}}$ et si l'envoyeur demande à $\mathcal{F}_{\text{1CC}}$ de dévoiler ce résultat, le receveur dévoile aussi la base accompagnant le résultat en ouvrant la mise en gage correspondante. Ce nouveau protocole ressemble au protocole pour $\mathcal{F}_{\text{OT}}$ dans le modèle $\mathcal{F}_{\text{2CC}}$-hybride présenté et prouvé UC-sûr dans [FKS+13], ce qui nous permet de réutiliser une partie de leur analyse.

Survol de la preuve

Pour montrer qu'un protocole Π implémente de manière sûre une fonctionnalité $\mathcal{F}$ dans le modèle UC, il faut montrer que pour tout adversaire Adv qui attaque le protocole Π en corrompant un des participants, il existe un simulateur Sim qui attaque plutôt la fonctionnalité $\mathcal{F}$, mais qui est indistinguable de Adv aux yeux d'un observateur externe Env. Plus précisément, on veut que le modèle réel où Adv interagit avec Π soit indistinguable du modèle idéal où Sim interagit avec $\mathcal{F}$ (voir figure 3.3). Pour une description plus détaillée du modèle UC, voir la section 2.4.

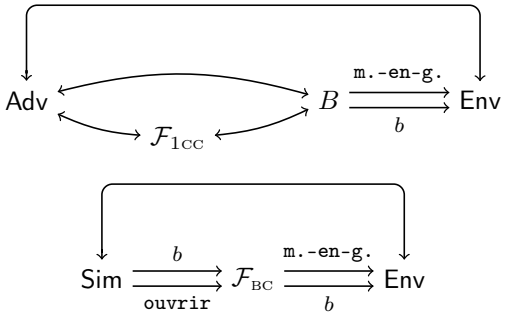


FIGURE 3.3 – Le modèle réel (dessus) et le modèle idéal (dessous) pour le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ et la fonctionnalité $\mathcal{F}_{\text{BC}}$, respectivement, avec Alice corrompue. La fonctionnalité $\mathcal{F}_{\text{BC}}$ est présentée à la figure 2.2.

La plupart des preuves dans le modèle UC suivent un même moule. Le simulateur Sim exécute intérieurement une copie de l'adversaire (de manière boîte noire) et simule les actions et interactions du participant honnête et des fonctionnalités idéales utilisées par le protocole. Sim doit offrir la même interface à Env que Adv, alors il fait suivre tout message entre l'environnement et (son instance interne

de) l'adversaire. Finalement, à partir des interactions de l'adversaire avec les fonctionnalités idéales et du participant honnête, il extrait les valeurs à entrer dans la fonctionnalité idéale externe (voir figure 3.4).

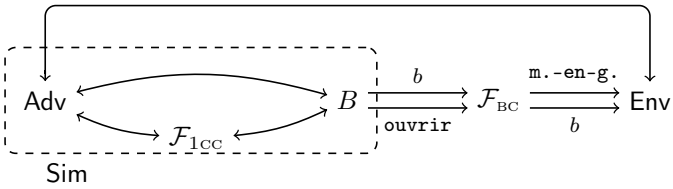


FIGURE 3.4 – La construction standard du simulateur Sim : exécuter Adv de manière interne et simuler les actions de Bob et de $\mathcal{F}_{\text{1CC}}$ honnêtement. Par les interactions entre ces trois partis, extraire les entrées à la fonctionnalité $\mathcal{F}_{\text{BC}}$ externe.

De plus, dans toutes les preuves ci-dessous, Sim simule le participant honnête en l'exécutant selon les actions décrites dans le protocole pour ce participant, à quelques modifications près qui seront indétectables du point de vue de l'adversaire, et qui n'affecteront pas la sortie de ce participant. Ainsi, le simulateur (dans le modèle idéal) construit de cette façon sera toujours indistinguable de l'adversaire (dans le modèle réel) du point de vue de Env, il suffira donc de montrer que la sortie du participant honnête (dans le modèle réel) est indistinguable de la sortie de la fonctionnalité idéale (dans le modèle idéal).

Nous procédons de la manière suivante pour montrer la UC-complétude de $\mathcal{F}_{\text{1CC}}$. D'abord, nous montrons la sécurité du protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ contre Alice corrompue (proposition 3.3.1). Ensuite, nous montrons que $\mathcal{F}_{\text{BC}}$ et $\mathcal{F}_{\text{1CC}}$ peuvent être utilisés ensemble pour implémenter $\mathcal{F}_{\text{2CC}}$ de manière UC-sûre par le protocole naturel $\Pi_{\text{2CC'}}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{\text{1CC}}}$ présenté dans la figure 3.5 (en réalité, on implémente une variante de la primitive2CC qu'on nomme 2CC' où l'envoyeur a l'option d'avorter après avoir vu l'entrée du receveur). La sûreté de ce protocole dans le modèle UC est établie par la proposition 3.3.2. En implémentant cette variante de $\mathcal{F}_{\text{2CC}}$ dans le modèle $\mathcal{F}_{\text{1CC}}$-hybride avec le protocole $\Pi_{\text{2CC'}}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{\text{1CC}}}$ où les instances de $\mathcal{F}_{\text{BC}}$ sont remplacées par des appels au protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$, on obtient un protocole pour $\mathcal{F}_{\text{2CC}}$ qui est sûr contre envoyeur corrompu. Ensuite, on utilise le fait que $\mathcal{F}_{\text{2CC}}$ implique $\mathcal{F}_{\text{OT}}$ par le biais du protocole $\hat{\Pi}_{\text{OT}}^{\mathcal{F}_{\text{2CC}}}$ défini et prouvé UC-sûr dans [FKS+13]. En utilisant l'implémentation de $\mathcal{F}_{\text{2CC}}$ définie plus haut dans $\hat{\Pi}_{\text{OT}}^{\mathcal{F}_{\text{2CC}}}$, on obtient un protocole $\Pi_{\text{OT}}^{\mathcal{F}_{\text{1CC}}}$ qui est UC-sûr contre un receveur corrompu (lemme 3.3.3). Finalement, il est assez simple de montrer que $\Pi_{\text{OT}}^{\mathcal{F}_{\text{1CC}}}$ est UC-sûr contre un envoyeur malhonnête de manière directe (lemme 3.3.4).

Réduction UC de $\mathcal{F}_{\text{OT}}$ à $\mathcal{F}_{\text{1CC}}$

Montrons d'abord la sûreté UC de notre protocole de mise en gage $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ contre Alice corrompue. Pour que le protocole imite la fonctionnalité $\mathcal{F}_{\text{BC}}$, nous faisons l'hypothèse que Bob produit la sortie `mise-en-gage` si et seulement s'il n'avorte pas le protocole durant la phase de mise en gage et qu'il produit la sortie (`ouvert`, b) si et seulement s'il n'avorte pas lorsqu'Alice tente d'ouvrir le bit b. Autrement dit, dès qu'il avorte, il ne produit aucune sortie.

Proposition 3.3.1. *Le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ implémente $\mathcal{F}_{\text{BC}}$ dans le modèle UC quantique contre envoyeuse Alice corrompue.*

Démonstration. La construction du simulateur Sim est comme suit. Le simulateur exécute intérieurement l'attaque d'Alice malhonnête, et simule les actions de Bob et de $\mathcal{F}_{\text{1CC}}$ de manière honnête. Notons que puisque Sim simule l'action des $\mathcal{F}_{\text{1CC}}$, il peut voir les entrées d'Alice aux boîtes $\mathcal{F}_{\text{1CC}}$. Lorsqu'Alice annonce g, w et s à la fin de la phase de mise en gage, Sim calcule $b = g(\theta') \oplus w$, où θ' est la chaine de syndrome s la plus près de la chaine $\theta_{\bar{t}}$ des valeurs entrées dans les $\mathcal{F}_{\text{1CC}}$ qui n'ont pas été reçus par Bob (c'est-à-dire pour lesquels son entrée à $\mathcal{F}_{\text{1CC}}$ était 0). Si Bob n'avorte pas la phase de mise en gage, Sim envoie l'entrée b dans la fonctionnalité $\mathcal{F}_{\text{BC}}$ externe. Finalement, lorsqu'Alice corrompue ouvre sa mise en gage à b', Sim entre `ouvrir` dans la fonctionnalité $\mathcal{F}_{\text{BC}}$ si Bob accepte l'ouverture du bit b', et n'entre rien si Bob a avorté.

Il découle directement du théorème 3.3.2 que le bit de sortie b' du Bob simulé est égal au bit b calculé par Sim et donné en entrée à la fonctionnalité $\mathcal{F}_{\text{BC}}$ externe, sauf avec probabilité négligeable. Ainsi, le modèle réel est statistiquement indistinguable du modèle idéal. □

Considérons le protocole $\Pi_{\text{2CC}}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{\text{1CC}}}$ présenté à la figure 3.5 qui se veut un candidat pour une implémentation de $\mathcal{F}_{\text{2CC}}$. La fonctionnalité idéale que ce protocole implémente ne correspond pas exactement à $\mathcal{F}_{\text{2CC}}$, mais plutôt à une variante de la primitive 2CC où Alice, après avoir reçu l'entrée $c \in \{0, 1\}$ de Bob, a l'option de l'empêcher d'obtenir le second bit de la sortie à laquelle il s'attendrait pour la primitive 2CC (soit (s_0, s_1) si $c = 1$ et $\perp$ si $c = 0$). Cette déviation de 2CC est due au fait qu'Alice, après avoir appris l'entrée de Bob à la boîte 1CC dans le protocole $\Pi_{\text{2CC}}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{\text{1CC}}}$, peut refuser d'ouvrir sa mise en gage, faisant en sorte que Bob n'apprenne pas les deux bits d'entrée d'Alice. Cette nouvelle primitive est décrite par le comportement d'entrée/sortie de la fonctionnalité $\mathcal{F}_{\text{2CC'}}$ illustré à la figure 3.6.

Ce détail de l'implémentation de $\Pi_{\text{2CC}}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{\text{1CC}}}$ n'influencera pas la sécurité de notre protocole pour OT ; puisque Bob sait quand Alice refuse d'ouvrir sa mise en gage, il pourra avorter le protocole pour OT dès qu'elle refuse d'« ouvrir » un des $\mathcal{F}_{\text{2CC'}}$. Donc en pratique, la primitive 2CC' se permet la réalisation de la

primitive 2CC.

Participants : L'envoyeuse Alice et le receveur Bob.

Entrées : Alice reçoit $s_0, s_1 \in \{0,1\}$ et $a \in \{0,1\}$, et Bob reçoit $c \in \{0,1\}$.

1. Alice entre s_1 dans $\mathcal{F}_{\text{BC}}$, Bob reçoit le message `mise-en-gage`.
2. Alice et Bob font appel à $\mathcal{F}_{1\text{CC}}$ avec entrées s_0 et c, respectivement. Alice reçoit c de $\mathcal{F}_{1\text{CC}}$ et Bob reçoit s_0.
3. Bob produit la sortie s_0 si $c = 1$ et $\perp$ sinon. Alice produit la sortie c.
4. Sur sa seconde entrée a, Alice ne fait rien si $a = 1$. Si $a = 0$, elle envoie le message `ouvrir` à $\mathcal{F}_{\text{BC}}$ si $c = 1$, auquel cas Bob reçoit s_1 de $\mathcal{F}_{1\text{CC}}$ et ne fait rien si $c = 0$.
5. Bob produit la sortie s_1 si Alice a ouvert sa mise en gage.

FIGURE 3.5 – Le protocole $\Pi_{\text{2CC'}}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{1\text{CC}}}$. Ce protocole implémente une variante de 2CC où Alice a le pouvoir d'avorter après avoir appris l'entrée de Bob (voir figure 3.6).

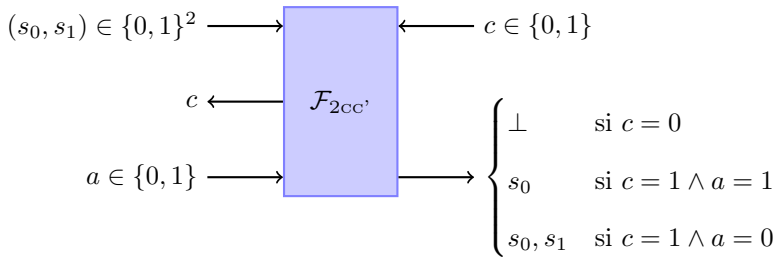


FIGURE 3.6 – La fonctionnalité $\mathcal{F}_{\text{2CC'}}$. Alice (à gauche) est l'envoyeuse et Bob (à droite) est le receveur. Les messages sont envoyés séquentiellement du haut vers le bas : Alice entre ses deux bits s_0, s_1 et Bob son bit de sélection c, Alice apprend c et peut répondre par un bit a qui indique si Bob recevra ou non l'entrée s_1.

Proposition 3.3.2. *Le protocole* $\Pi_{\text{2CC'}}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{1\text{CC}}}$ *implémente* $\mathcal{F}_{\text{2CC'}}$ *dans le modèle UC.*

Démonstration. Nous considérons d'abord le cas d'Alice corrompue. Le simulateur Sim simule les actions et interactions de Bob, $\mathcal{F}_{\text{BC}}$ et $\mathcal{F}_{1\text{CC}}$ en les faisant agir de manière honnête. À l'étape 2, lorsque Sim apprend les entrées respectives s_0 et s_1 d'Alice aux fonctionnalités $\mathcal{F}_{\text{BC}}$ et $\mathcal{F}_{1\text{CC}}$, il entre (s_0, s_1) dans la fonctionnalité $\mathcal{F}_{\text{2CC'}}$ externe. Après avoir reçu c de la fonctionnalité $\mathcal{F}_{\text{2CC'}}$ externe, Sim envoie c à Bob pour qu'il le donne en entrée dans la boîte $\mathcal{F}_{1\text{CC}}$. Si $c = 0$, alors Bob simulé et 2CC′ produisent tous deux la sortie $\perp$. Si $c = 1$, alors Bob et 2CC' produiront tous deux la sortie s_0. Par la suite, si Alice ouvre sa mise en gage, c'est-à-dire si Bob simulé produit sa seconde sortie s_1, Sim entrera $a = 0$ dans $\mathcal{F}_{\text{2CC'}}$, auquel

cas la fonctionnalité $\mathcal{F}_{\text{2CC}'}$ externe produira la même sortie s_0, s_1 que Bob. Nous venons d'établir la sûreté du protocole contre Alice corrompue puisque dans tous les cas, la sortie de Bob honnête (dans le monde réel) et de la fonctionnalité externe $\mathcal{F}_{\text{2CC}'}$ (dans le monde idéal) sont identiques.

La sécurité contre Bob corrompu est aussi facile à prouver. Sim simule Alice, $\mathcal{F}_{\text{BC}}$ et $\mathcal{F}_{\text{1CC}}$ de manière honnête : sur entrée s_0 et s_1, Alice entre s_1 dans $\mathcal{F}_{\text{BC}}$ et entre s_0 dans $\mathcal{F}_{\text{1CC}}$, produit la sortie c lorsqu'elle le reçoit de $\mathcal{F}_{\text{1CC}}$ et sur entrée a, envoie le message `ouvrir` à $\mathcal{F}_{\text{BC}}$ si et seulement si $c = 1$ et $a = 0$. La sortie d'Alice dans le monde réel est évidemment indistinguable de la sortie de $\mathcal{F}_{\text{2CC}'}$ dans le monde idéal. Il reste à montrer que Bob corrompu apprend la même information dans les mondes réel et idéal. Il suffit d'analyser les trois cas qui sont tous faciles à vérifier :

— si $c = 0$, Bob simulé et réel n'apprennent rien sur s_0, s_1 ou a,

— si $a = 1$ et $c = 1$, Bob simulé et réel apprennent s_0, mais pas s_1, et

— si $a = 0$ et $c = 1$, Bob simulé et réel apprennent s_0 et s_1.

L'information sur a que Bob apprend du protocole dans le monde réel est aussi la même qui peut être inférée de la sortie de $\mathcal{F}_{\text{2CC}'}$ dans le monde idéal. □

En utilisant le fait que notre protocole de mise en gage $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ implémente $\mathcal{F}_{\text{BC}}$ de manière sûre dans le modèle UC quantique contre envoyeuse Alice corrompue (proposition 3.3.1), on obtient immédiatement un protocole pour $\mathcal{F}_{\text{2CC}'}$ dans le modèle $\mathcal{F}_{\text{1CC}}$-hybride qui est sûr contre Alice corrompue en remplaçant l'appel à $\mathcal{F}_{\text{BC}}$ du protocole $\Pi_{\text{2CC}'}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{\text{1CC}}}$ par $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$.

Corollaire 3.3.1. *Le protocole $\Pi_{\text{2CC}'}^{\mathcal{F}_{\text{1CC}}}$, défini en remplaçant l'appel à $\mathcal{F}_{\text{BC}}$ par le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{\text{1CC}}}$ dans le protocole $\Pi_{\text{2CC}'}^{\mathcal{F}_{\text{BC}},\mathcal{F}_{\text{1CC}}}$, implémente $\mathcal{F}_{\text{2CC}'}$ de manière sûre dans le modèle UC quantique contre envoyeuse Alice corrompue.*

Nous sommes maintenant prêts à présenter le protocole $\Pi_{\text{OT}}^{\mathcal{F}_{\text{1CC}}}$ de transfert équivoque dans le modèle $\mathcal{F}_{\text{1CC}}$-hybride que nous prouverons sûr dans le modèle UC quantique. Ce protocole, présenté à la figure 3.7, est identique au protocole pour OT dans le modèle $\mathcal{F}_{\text{2CC}}$-hybride présenté dans [FKS+13], à l'exception près que les appels à $\mathcal{F}_{\text{2CC}}$ ont été remplacés par le protocole $\Pi_{\text{2CC}'}^{\mathcal{F}_{\text{1CC}}}$ défini au corollaire 3.3.1.

Lemme 3.3.3. *Le protocole $\Pi_{\text{OT}}^{\mathcal{F}_{\text{1CC}}}$ implémente $\mathcal{F}_{\text{OT}}$ de manière sûre dans le modèle UC quantique contre receveur Bob corrompu.*

Démonstration. Notons que les étapes 3a à 3c du protocole $\Pi_{\text{OT}}^{\mathcal{F}_{\text{1CC}}}$ sont identiques au protocole $\Pi_{\text{2CC}'}^{\mathcal{F}_{\text{1CC}}}$ défini par le corollaire 3.3.1 ci-dessus avec Bob comme envoyeur et Alice comme receveuse [5]. Puisque $\Pi_{\text{2CC}'}^{\mathcal{F}_{\text{1CC}}}$ implémente $\mathcal{F}_{\text{2CC}'}$ contre envoyeur corrompu de manière UC-sûre (corollaire 3.3.1), on peut remplacer les

5. Les rôles habituels sont ici inversés.

étapes 3a à 3c par un appel à la fonctionnalité idéale $\mathcal{F}_{2\text{CC'}}$ avec Bob comme envoyeur et Alice comme receveuse, et ainsi obtenir un protocole $\Pi_{\text{OT}}^{\mathcal{F}_{2\text{CC'}}}$ dans le modèle $\mathcal{F}_{2\text{CC'}}$-hybride qui est aussi sûr que $\Pi_{\text{OT}}^{\mathcal{F}_{1\text{CC}}}$ contre un receveur Bob (l'envoyeur du 2CC') corrompu. Il nous suffit donc d'établir la sûreté UC de $\Pi_{\text{OT}}^{\mathcal{F}_{2\text{CC'}}}$ contre receveur corrompu pour établir la sûreté de $\Pi_{\text{OT}}^{\mathcal{F}_{1\text{CC}}}$.

La seule différence entre le protocole $\Pi_{\text{OT}}^{\mathcal{F}_{2\text{CC'}}}$ décrit ci-dessus et le protocole $\hat{\Pi}_{\text{OT}}^{\mathcal{F}_{2\text{CC}}}$ de [FKS+13] dans le modèle $\mathcal{F}_{2\text{CC}}$-hybride est que notre protocole utilise la primitive 2CC' au lieu de 2CC. Cette différence se réduit donc à la différence entre 2CC et 2CC' qui est que l'envoyeur a l'option d'empêcher le receveur d'obtenir le deuxième bit s_1. Cette différence n'affecte pas la sûreté du protocole pour la raison suivante : tout adversaire contre $\Pi_{\text{OT}}^{\mathcal{F}_{2\text{CC'}}}$ qui fait avorter l'envoyeur Bob dans une des boîtes $\mathcal{F}_{2\text{CC'}}$ (c'est-à-dire qui entre $a = 1$ dans 2CC') est parfaitement indistinguable d'un adversaire contre $\hat{\Pi}_{\text{OT}}^{\mathcal{F}_{2\text{CC}}}$ qui fait avorter Bob *après* l'appel au $\mathcal{F}_{2\text{CC}}$ correspondant. La sûreté du protocole $\Pi_{\text{OT}}^{\mathcal{F}_{2\text{CC'}}}$ décrit ci-dessus contre receveur corrompu découle donc directement de la preuve de sûreté de $\hat{\Pi}_{\text{OT}}^{\mathcal{F}_{2\text{CC}}}$ qui se trouve dans [FKS+13] avec le simulateur légèrement modifié pour accommoder la différence entre 2CC et 2CC'. Ceci implique aussi la sûreté de $\Pi_{\text{OT}}^{\mathcal{F}_{1\text{CC}}}$ contre receveur corrompu. □

Lemme 3.3.4. *Le protocole $\Pi_{\text{OT}}^{\mathcal{F}_{1\text{CC}}}$ implémente $\mathcal{F}_{\text{OT}}$ de manière sûre dans le modèle UC quantique contre envoyeuse Alice corrompue.*

Démonstration. Pour une envoyeuse Alice corrompue et receveur Bob honnête, on définit le simulateur Sim de la manière suivante. Sim simule les actions de Bob et de 1CC de manière honnête, à une exception près. Le Bob simulé *ne* mesure *pas* les états qu'il reçoit à l'étape 2 du protocole, mais conserve les qubits reçus. Plus tard, dans l'étape 3b, à chaque fois qu'Alice entre $t_i = 1$ dans la fonctionnalité $\mathcal{F}_{1\text{CC}}$, Bob mesure le i^{e} qubit dans la base θ_i^B (la base à laquelle il s'est mis en gage) et entre le résultat x_i^B dans $\mathcal{F}_{1\text{CC}}$. Ce comportement est parfaitement indistinguable des actions normales de Bob et fait en sorte qu'après l'étape 3 du protocole, tous les qubits de Bob qui n'ont pas été vérifiés sont intacts.

Par la suite, à l'étape 5, Sim répond à Alice avec une partition aléatoire (I_0, I_1). À la fin du protocole, Sim mesure les qubits restants de Bob dans la base $\hat{\theta}^A$ dévoilée par Alice afin d'obtenir $\hat{x}^B = \hat{x}^A$. Sim peut donc calculer s_0 et s_1 et les introduire dans la fonctionnalité idéale $\mathcal{F}_{\text{OT}}$ externe. La sortie s_c de la fonctionnalité $\mathcal{F}_{\text{OT}}$ coïncide avec la chaine que Bob honnête aurait produite en sortie dans le modèle réel. On conclut donc que les modèles réel et idéal sont indistinguables. □

Théorème 3.3.3. *La fonctionnalité $\mathcal{F}_{1\text{CC}}$ est UC-complète dans le monde quantique.*

Démonstration. Nous avons montré que $\Pi_{\text{OT}}^{\mathcal{F}_{1\text{CC}}}$ implémente de manière sûre $\mathcal{F}_{\text{OT}}$ dans le modèle UC quantique par les lemmes 3.3.3 et 3.3.4. Donc $\mathcal{F}_{\text{OT}} \sqsubseteq \mathcal{F}_{1\text{CC}}$ et, puisque $\mathcal{F}_{\text{OT}}$ est complète pour le modèle UC quantique (théorème 2.4.1), $\mathcal{F}_{1\text{CC}}$ est aussi complète pour le modèle UC quantique. □

Paramètres : $\ell, n \geq 1$ et une famille $\mathcal{F}$ de fonctions de hachage 2-universelles de la forme $\{0,1\}^n \to \{0,1\}^\ell$.

Participants : L'envoyeuse Alice et le receveur Bob.

Entrées : Alice reçoit $s_0, s_1 \in \{0,1\}^\ell$ et Bob reçoit $c \in \{0,1\}$.

1. Alice choisit aléatoirement $x^A \in_R \{0,1\}^n$ et $\theta^A \in_R \{0,1\}^n$ et envoie l'état $H^{\otimes\theta^A}|x^A\rangle$ à Bob.
2. Sur réception, Bob choisit $\theta^B \in_R \{0,1\}^n$ et mesure l'état reçu dans la base θ^B. Soit $x^B \in \{0,1\}^n$ le résultat de cette mesure.
3. Pour $i = 1 \ldots n$,
   (a) Alice et Bob font appel au protocole $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$ avec Bob comme envoyeur et entrée θ_i^B.
   (b) Alice choisit un bit de sélection $t_i \in_R \{0,1\}$ et ils invoquent une instance de $\mathcal{F}_{1\text{CC}}$ avec Bob comme envoyeur et avec les entrées t_i et x_i^B pour Alice et Bob, respectivement.
   (c) Si Bob reçoit $t_i = 1$, il ouvre la i^{e} mise en gage en utilisant le protocole $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$.
4. Si pour un certain i tel que $t_i = 1$ il advient que $\theta_i^A = \theta_i^B$, mais que $x_i^B \neq x_i^A$, Alice avorte le protocole. Bob avorte si $t_i = 1$ pour plus de $3n/5$ positions. Soit $\hat{x}^A$ (respectivement $\hat{\theta}^A, \hat{x}^B, \hat{\theta}^B$) la restriction de x^A (respectivement θ^A, x^B, θ^B) aux positions i pour lesquelles $t_i = 0$.
5. Alice envoie $\hat{\theta}^A$ à Bob. Bob construit les ensembles $I_c = \{i : \hat{\theta}_i^A = \hat{\theta}_i^B\}$ et $I_{1-c} = \{i : \hat{\theta}_i^A \neq \hat{\theta}_i^B\}$, puis envoie (I_0, I_1) à Alice.
6. Alice choisit $f \in_R \mathcal{F}$, calcule $m_i = s_i \oplus f(x_i')$ où x_i' est la chaine de n bits produite en ajoutant suffisamment de zéros à $\hat{x}_{I_i}^A$ (pour $i = 0, 1$) et envoie (f, m_0, m_1) à Bob.
7. Bob produit la sortie $s = m_c \oplus f(x')$ où x' est la chaine de n bits produite en ajoutant suffisamment de zéros à $\hat{x}_{I_c}^B$.

FIGURE 3.7 – Le protocole $\Pi_{\text{OT}}^{\mathcal{F}_{1\text{CC}}}$. La primitive exacte qu'elle implémente est une variante de OT où les entrées d'Alice sont des chaines de ℓ bits. Pour $\ell = 1$, on retrouve la primitive OT telle que définie à la section 2.4.

3.4 Sûreté du protocole de mise en gage BCJL dans le modèle à mémoire bornée

Dans cette section, nous montrons que pour une classe importante de protocoles de mise en gage, la sécurité du protocole contre un envoyeur malhonnête, dans une version quelque peu renforcée du *modèle à mémoire quantique bornée*, se réduit à sa sécurité contre un envoyeur malhonnête qui n'a *aucune mémoire quantique*. Nous montrons ensuite comment ce résultat général s'applique à un protocole concret, le protocole de mise en gage BCJL [BCJL93].

3.4.1 Protocoles de mise en gage non interactifs

La classe de protocoles de mise en gage auxquels notre réduction s'applique est composée des protocoles qui sont *non interactifs* ; toute communication va d'Alice vers Bob, où Alice se met en gage et Bob est le receveur. De plus, on demande de la procédure de vérification du receveur d'être une mesure *projective*. Cette classe de protocoles est capturée par la définition suivante.

Définition 3.4.1. On dit qu'un protocole de mise en gage est *non interactif avec vérification projective*, s'il est de la forme suivante.

Mise en gage : Alice envoie un message classique x et un registre quantique B à Bob.

Ouverture de b : Alice envoie un message d'ouverture classique y_b à Bob, et Bob applique une mesure projective à résultat binaire $\{\mathbb{V}_{x,y_b}, \mathbb{1} - \mathbb{V}_{x,y_b}\}$ au registre B.

Puisque x est fixé après la phase de mise en gage, nous allons laisser implicite la dépendance sur x de $\mathbb{V}_{x,y_b}$, et nous écrirons donc $\mathbb{V}_{y_b}$. Aussi, pour éviter de trop encombrer le texte, nous utiliserons simplement le terme *non interactifs* pour parler de protocoles qui satisfont la définition 3.4.1.

Nous considérons la sécurité — plus précisément, la propriété *contraignante* — de tels protocoles dans une variante légèrement renforcée du modèle à mémoire quantique bornée [DFSS08, DFSS07, Sch07] où, en plus de la borne sur la mémoire quantique d'Alice, on requiert aussi que la mesure qui produit y_b pour la phase d'ouverture soit *projective*. Cette restriction est justifiée par le fait que les mesures générales (non projectives) nécessitent de la mémoire quantique additionnelle, sous forme de qubits ancillaires, pour être exécutées de manière cohérente par un circuit quantique. En effet, les mesures les plus générales, les POVM, sont équivalentes à une mesure projective sur un plus grand système qui a subi une évolution unitaire (théorème 2.3.5). D'un point de vue technique, cette restriction (ainsi que celle sur la mesure de Bob) est une conséquence de notre technique de preuve qui nécessite que la mesure conjointe d'Alice et

Bob dans la phase de mise en gage soit *répétable*. Éliminer cette restriction de notre preuve demeure une question ouverte. [6]

Formellement, nous représentons la propriété contraignante des protocoles de mise en gage non interactifs dans notre variante du modèle à mémoire bornée de la manière suivante.

Définition 3.4.2 (Propriété contraignante)**.** Un protocole de mise en gage non interactif est dit ϵ-*contraignant contre adversaires projectifs q-bornés* si, pour tout état $\rho_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ où $\dim(\mathcal{H}_{\mathsf{A}}) \leq 2^q$ et pour tout message classique x,

$$P_0^{\mathrm{A}}(\rho_{\mathsf{AB}}) + P_1^{\mathrm{A}}(\rho_{\mathsf{AB}}) \leq 1 + \epsilon \tag{3.13}$$

où

$$P_b^{\mathrm{A}}(\rho_{\mathsf{AB}}) := \max_{\{\mathbb{F}_{y_b}\}_{y_b}} \sum_{y_b} \mathrm{tr}\left((\mathbb{F}_{y_b} \otimes \mathbb{V}_{y_b})\rho_{\mathsf{AB}}\right)$$

est la probabilité d'ouvrir le bit b avec succès, maximisée sur toutes les mesures projectives $\{\mathbb{F}_{y_b}\}_{y_b}$.

Dans le cas $q = 0$, le critère ci-dessus se réduit à

$$P_0^{\mathrm{NA}}(\rho_{\mathsf{AB}}) + P_1^{\mathrm{NA}}(\rho_{\mathsf{AB}}) \leq 1 + \epsilon \quad \text{où} \quad P_b^{\mathrm{NA}}(\rho_{\mathsf{AB}}) := \max_{y_b} \mathrm{tr}\left(\mathbb{V}_{y_b}\rho_{\mathsf{B}}\right)$$

et où $\rho_{\mathsf{B}} = \mathrm{tr}_{\mathsf{A}}(\rho_{\mathsf{AB}})$, on parle alors de protocoles ϵ-contraignants contre adversaires *non adaptés*.

Sur le critère contraignant des protocoles de mise en gage non interactifs

Les critères de sécurité analogues à celui de la définition 3.4.2 (soit les critères de la forme $p_0+p_1 \leq 1+\epsilon$) ont traditionnellement été des notions de sécurité faibles contre les metteurs en gage malhonnêtes, par opposition à des définitions qui sont plus dans l'esprit de l'existence d'un bit qui ne peut pas être ouvert par l'adversaire. Bien qu'il soit plus facile de prouver la sécurité avec cette définition, un défaut notoire de la définition $p_0 + p_1 \leq 1 + \epsilon$ est qu'elle n'interdit pas la situation suivante. Un adversaire pourrait, par une mesure complexe, soit complètement ruiner sa probabilité d'ouvrir la mise en gage, soit être capable d'ouvrir le bit de son choix. Alors les probabilités d'ouvrir 0 et 1 somment à un, mais conditionné sur le second résultat de cette mesure, elles somment à 2. C'est évidemment une propriété indésirable d'un protocole de mise en gage quantique.

Les protocoles de mise en gage non interactifs qui sont sûrs selon la définition 3.4.2 sont contraignants dans un sens plus fort. Par exemple, le problème présenté ci-dessus avec les définitions de type $p_0+p_1 \leq 1+\epsilon$ n'est pas applicable dans le cas de protocoles non interactifs. Si un protocole est ϵ-contraignant, alors *pour*

6. La technique standard, c'est-à-dire d'utiliser le théorème de Naimark (théorème 2.3.5), ne semble pas fonctionner dans notre cas.

tout état ρ (potentiellement obtenu en post-sélectionnant sur un résultat de mesure) doit satisfaire (3.13). Si la somme des deux probabilités d'ouvrir 0 et 1 était plus grande que $1+\epsilon$ pour un état particulier $\bar{\rho}$ obtenu par post-sélection, l'adversaire aurait pu préparer cet état en premier lieu, contredisant ainsi la supposition que le protocole est ϵ-contraignant.

C'est une question ouverte que de définir plus précisément la notion de sécurité des protocoles non interactifs qui satisfont la définition 3.4.2. En particulier, comment cette notion peut être reliée à une définition en termes de l'existence d'un bit qui ne peut pas être ouvert, sauf avec probabilité négligeable, par exemple comme il est fait dans [FF16] pour le cas général (c'est-à-dire pour les protocoles possiblement interactifs).

3.4.2 La réduction générale

Nous voulons réduire la sécurité d'un protocole non interactif contre un adversaire projectif q-borné à sa sécurité contre un adversaire non adapté ($q=0$) qui, en général, est plus facile à prouver. Pour ce faire, nous utilisons notre réduction des adversaires adaptés aux adversaires non adaptés (corollaire 3.2.1), mais notre relation A-vs-NA ne s'applique pas directement. Nous avons besoin d'un outil supplémentaire donné par le lemme suivant. Il établit le fait que s'il existe une stratégie de mise en gage pour Alice telle que la probabilité cumulative d'ouvrir 0 et 1 excède 1 par une quantité non négligeable, alors il existe aussi une stratégie de mise en gage qui fait en sorte qu'elle puisse ouvrir 0 *avec certitude*, mais qu'elle puisse aussi ouvrir 1 avec probabilité non négligeable.

Lemme 3.4.1. *Soient* $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ *et* $\epsilon > 0$ *tels que* $P_0^{\mathrm{A}}(\rho) + P_1^{\mathrm{A}}(\rho) \geq 1+\epsilon$. *Alors, il existe* $\rho^0 \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}})$ *tel que* $P_0^{\mathrm{A}}(\rho^0) = 1$ *et* $P_1^{\mathrm{A}}(\rho^0) \geq \epsilon^2$.

Démonstration. Soit $\{\mathbb{F}_{y_0}\}_{y_0}$ et soit $\{\mathbb{G}_{y_1}\}_{y_1}$ des mesures projectives sur le registre A et qui maximisent respectivement les valeurs $P_0^A(\rho)$ et $P_1^A(\rho)$. Définissons les opérateurs de projection sur les sous-espaces acceptant respectivement les ouvertures à 0 et à 1 comme

$$\mathbb{P}_0 := \sum_{y_0} \mathbb{F}_{y_0} \otimes \mathbb{V}_{y_0} \text{ et } \mathbb{P}_1 := \sum_{y_1} \mathbb{G}_{y_1} \otimes \mathbb{V}_{y_1} \ .$$

Puisque $\mathrm{tr}((\mathbb{P}_0+\mathbb{P}_1)\rho) = P_0^{\mathrm{A}}(\rho) + P_1^{\mathrm{A}}(\rho) \geq 1+\epsilon$, on peut déduire que $\|\mathbb{P}_0+\mathbb{P}_1\|_\infty \geq 1+\epsilon$. Autrement dit, la plus petite valeur propre de $\mathbb{P}_0+\mathbb{P}_1$ dépasse $1+\epsilon$. Par le lemme 2.3.1, on a que

$$1 + \|\mathbb{P}_1\mathbb{P}_0\|_\infty \geq \|\mathbb{P}_0+\mathbb{P}_1\|_\infty \geq 1+\epsilon \ .$$

L'inégalité ci-dessus implique l'existence d'un état normalisé $|\phi\rangle$ tel que $\|\mathbb{P}_1\mathbb{P}_0|\phi\rangle\| \geq \epsilon$ par la définition de la norme spectrale (équation (2.24)). Définissons alors $|\phi_0\rangle := \mathbb{P}_0|\phi\rangle / \|\mathbb{P}_0|\phi\rangle\|$ qui a les propriétés requises :

la probabilité d'ouvrir 0 à partir de l'état $|\phi_0\rangle$ est $\mathrm{tr}(\mathbb{P}_0|\phi_0\rangle\langle\phi_0|) = \||\mathbb{P}_0|\phi_0\rangle\|^2 = 1$, et la probabilité d'ouvrir 1 à partir du même état est

$$\mathrm{tr}\left(\mathbb{P}_1|\phi_0\rangle\langle\phi_0|\right) = \||\mathbb{P}_1|\phi_0\rangle\|^2 = \|\mathbb{P}_1\mathbb{P}_0|\phi\rangle\|^2 \,/\, \|\mathbb{P}_0|\phi\rangle\|^2 \geq \epsilon^2 \ . \qquad \square$$

Nous sommes maintenant prêts à énoncer et à prouver la réduction générale des adversaires projectifs q-bornés aux adversaires non adaptés.

Théorème 3.4.1. *Si un protocole de mise en gage non interactif est ϵ-contraignant contre les adversaires non adaptés, alors il est $\sqrt{2^q\epsilon}$-contraignant contre les adversaires projectifs q-bornés.*

Démonstration. Soit $\rho_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B})$ l'état conjoint d'Alice et Bob où $\dim(\mathcal{H}_\mathsf{A}) \leq 2^q$ et soit $\alpha > 0$ tel que les probabilités d'ouverture de 0 et 1 satisfont $P_0^A(\rho) + P_1^A(\rho) = 1 + \alpha$. Par le lemme 3.4.1, on sait qu'il existe $\rho^0_{\mathsf{AB}} \in \mathcal{D}(\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B})$ construit à partir de ρ_{AB} tel que

$$P_0^A(\rho^0) = 1 \text{ et } P_1^A(\rho^0) \geq \alpha^2 \ .$$

Utilisons le corollaire 3.2.1 et la supposition que le protocole est ϵ-contraignant contre les adversaires non adaptés pour montrer que α ne peut pas être trop grand. Soit $\{\mathbb{F}_{y_0}\}_{y_0}$ une mesure telle que $\sum_{y_b} \mathrm{tr}((\mathbb{F}_{y_b} \otimes \mathbb{V}_{y_b})\rho_{\mathsf{AB}}) = P_0^A(\rho^0) = 1$. Considérons l'état réduit du registre B de ρ^0_{AB} :

$$\rho^0_\mathsf{B} = \mathrm{tr}_\mathsf{A}\left(\rho^0_{\mathsf{AB}}\right) = \sum_{y_0} \mathrm{tr}_\mathsf{A}\left((\mathbb{F}_{y_0} \otimes \mathbb{1}_\mathsf{B})\rho^0_{\mathsf{AB}}\right) = \sum_{y_0} \lambda_{y_0}\sigma^{y_0}_\mathsf{B}$$

où $\lambda_{y_0} := \mathrm{tr}((\mathbb{F}_{y_0} \otimes \mathbb{1}_\mathsf{B})\rho^0_{\mathsf{AB}})$ et $\sigma^{y_0}_\mathsf{B} := \lambda_{y_0}^{-1}\,\mathrm{tr}_\mathsf{A}((\mathbb{F}_{y_0} \otimes \mathbb{1}_\mathsf{B})\rho^0_{\mathsf{AB}})$. Pour chaque y_0, on a que $\mathrm{tr}(\mathbb{V}_{y_0}\sigma^{y_0}_\mathsf{B}) = 1$ par construction de ρ^0_{AB}. Ceci implique que $\mathrm{tr}(\mathbb{V}_{y_1}\sigma^{y_0}_\mathsf{B}) \leq \epsilon$ pour chaque y_1 qui ouvre 1 par la supposition que le protocole est ϵ-contraignant contre adversaires non adaptés. Alors on a

$$P_1^{\mathrm{NA}}(\rho^0_{\mathsf{AB}}) = \max_{y_1} \mathrm{tr}\left(\mathbb{V}_{y_1}\rho^0_\mathsf{B}\right) = \max_{y_1} \sum_{y_0} \lambda_{y_0}\,\mathrm{tr}\left(\mathbb{V}_{y_1}\sigma^{y_0}_\mathsf{B}\right) \leq \epsilon \ .$$

En appliquant le corollaire 3.2.1, on obtient la borne suivante sur α :

$$\alpha^2 \leq P_1^{\mathrm{A}}(\rho^0) \leq 2^{\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho_0}} P_1^{\mathrm{NA}}(\rho^0) \leq 2^{\mathrm{H}_0(\mathsf{A})_{\rho_0}}\epsilon \leq 2^q\epsilon \ . \qquad \square$$

3.4.3 Cas spécial : le protocole de mise en gage BCJL

Dans cette section, nous utilisons les résultats que nous venons de présenter pour montrer la sécurité du protocole de mise en gage BCJL (voir figure 3.8) dans le modèle défini par la définition 3.4.1.

Le protocole BCJL cache la valeur du bit mis en gage par l'utilisation d'une famille 2-universelle de fonctions de hachage appliquées sur le mot de code d'un code correcteur, mot de code qui est transmis

par le biais de l'encodage BB84. L'idée derrière cette technique est que l'amplification de l'incertitude cache le bit mis en gage tant qu'il y a suffisamment d'incertitude sur le mot de code, tandis que le code correcteur fait en sorte qu'il soit difficile de changer la valeur de ce bit sans être détecté.

Le protocole décrit à la figure 3.8 diffère légèrement du protocole original [BCJL93] dans le choix des paramètres et la tolérance au bruit de transmission. Cette différence est superficielle et nous permettra de recycler des éléments de l'analyse de la section 3.3. La tolérance au bruit de transmission peut être prise en compte en utilisant des techniques standards [BCJL93, Sch07].

MISE-EN-GAGE(b) :

1. Soit $\mathcal{C}$ un code correcteur linéaire $[n, k, d]$ où $k > 0.78n$.
2. Alice choisit aléatoirement une chaine $x \in_R \{0,1\}^n$ et une base $\theta \in_R \{0,1\}^n$. Elle envoie $H^{\otimes\theta}|x\rangle$ à Bob.
3. À la réception des qubits, Bob choisit une base aléatoire $\hat{\theta} \in_R \{0,1\}^n$ et mesure les qubits reçus dans la base $\hat{\theta}$. Soit $\hat{x}$ le résultat de sa mesure.
4. Soit $\mathcal{F}$ une famille 2-universelle de fonctions de hachage de la forme $\{0,1\}^n \to \{0,1\}$. Alice choisit $f \in_R \mathcal{F}$ et calcule le syndrome s de x pour le code correcteur $\mathcal{C}$. Elle envoie $w = f(x) \oplus b$, f et s à Bob.

OUVERTURE :

1. Alice envoie x, θ et b à Bob.
2. Bob vérifie que x a comme syndrome s. Il vérifie ensuite que $\hat{x}_i = x_i$ pour tout i tel que $\hat{\theta}_i = \theta_i$. Il accepte si $g(x) \oplus w = b$ et qu'aucun des tests ci-dessus n'a échoué.

FIGURE 3.8 – Le protocole de mise en gage BCJL.

Pour la sécurité contre le receveur Bob malhonnête, nous utilisons la même définition de camouflant qu'à la section 3.3 (définition 3.3.1). La preuve que le protocole BCJL satisfait cette définition est essentiellement la même que la preuve de sécurité contre Bob du protocole $\Pi_{\text{BC}}^{\mathcal{F}_{1\text{CC}}}$ de la section 3.3.

Théorème 3.4.2. *Le protocole* BCJL *est* $2^{0.01n}$*-camouflant selon la définition 3.3.1.*

Démonstration. Pour montrer que la fonction de hachage f appliquée à x camoufle le bit b, il faut montrer que x a suffisamment de min-entropie pour appliquer le théorème d'amplification de l'incertitude (théorème 2.6.1). D'abord, la probabilité que Bob devine la valeur d'un bit de x est la probabilité maximale de

distinguer les états

$$\sigma_0 := \frac{1}{2}\left(|0\rangle\langle 0| + |+\rangle\langle +|\right) \text{ et } \sigma_1 := \frac{1}{2}\left(|1\rangle\langle 1| + |-\rangle\langle -|\right) \ .$$

Cette probabilité est donnée par $\gamma := \frac{1}{2} + \frac{1}{2}\left\|\sigma_0 - \sigma_1\right\|_1 = \cos^2(\pi/8) \approx 0.85$ selon le théorème d'Helström. Donc la probabilité de deviner la valeur de x est γ^n. Comme f est indépendant de x, l'information sur x que Bob gagne par l'annonce des informations classiques est d'au plus la taille de s, par la règle de chaine pour la min-entropie (théorème 2.5.1). Puisque la taille de s est de $n-k$ bits, on peut conclure que la min-entropie de Bob sur x est d'au moins $n \log \frac{1}{\gamma} - (n-k) \approx (0.23 - 0.22)n = 0.01n$. □

Au lieu de montrer que BCJL est contraignant, nous allons montrer qu'un protocole équivalent BCJL$_\delta$ (voir figure 3.9) est contraignant. Le protocole BCJL$_\delta$ est une version modifiée de BCJL dans laquelle Bob a une mémoire quantique illimitée et garde les qubits envoyés par Alice en mémoire au lieu de les mesurer. Bob mesurera ces qubits à l'ouverture seulement et acceptera s'il n'observe pas trop d'erreurs dans l'annonce d'Alice. La phase d'ouverture de BCJL$_\delta$ est paramétrée par $\delta > 0$ qui détermine le taux d'erreur toléré par Bob et donc à quel point ce protocole se comporte comme BCJL. Le lemme suivant montre que les deux protocoles sont (presque) équivalents du point de vue d'Alice, c'est-à-dire que si Alice peut tricher contre BCJL, alors elle peut aussi tricher contre BCJL$_\delta$.

MISE-EN-GAGE$_\delta(b)$:

1. Soit $\mathcal{C}$ un code correcteur linéaire $[n,k,d]$ où $k > 0.78n$.
2. Alice choisit aléatoirement une chaine $x \in_R \{0,1\}^n$ et une base $\theta \in_R \{0,1\}^n$. Elle envoie $H^{\otimes\theta}|x\rangle$ à Bob.
3. À la réception des qubits, Bob les garde en mémoire pour les mesurer plus tard.
4. Soit $\mathcal{F}$ une famille 2-universelle de fonctions de hachage de la forme $\{0,1\}^n \to \{0,1\}$. Alice choisit $f \in_R \mathcal{F}$ et calcule le syndrome s de x pour le code correcteur $\mathcal{C}$. Elle envoie $w = f(x) \oplus b$, f et s à Bob.

OUVERTURE$_\delta$:

1. Alice envoie x, θ et b à Bob.
2. Bob vérifie que x a comme syndrome s. Il mesure ensuite les qubits qu'il a gardés en mémoire dans la base θ et obtient le résultat $\hat{x}$. Il accepte si $d(x,\hat{x}) \leq \delta n$ et $f(x) \oplus w = b$ et rejette sinon.

FIGURE 3.9 – Le protocole de mise en gage BCJL$_\delta$

Lemme 3.4.2. *Soit $\delta > 0$. Si le protocole* BCJL$_\delta$ *est ϵ-contraignant selon la définition 3.4.2, alors* BCJL *est $(\epsilon + 2^{-\delta n+1})$-contraignant.*

Démonstration. Supposons qu'Alice et Bob ont précédemment exécuté la phase de mise en gage du protocole BCJL avec valeurs w, g et s envoyées à Bob. Soit x et θ les valeurs envoyées par Alice au début de la phase d'ouverture et supposons s.p.d.g. que ces valeurs ouvrent le bit $b = 0$. Notons d'abord que les actions de Bob dans le protocole BCJL sont équivalentes à garder les qubits en mémoire à leur réception, mesurer ces qubits dans la base θ dans la phase d'ouverture pour obtenir $\hat{x}$ et vérifier que $x_T = \hat{x}_T$ pour un échantillon aléatoire uniformément distribué $T \subseteq_R [n]$. De ce point de vue, le résultat de mesure de Bob est identiquement distribué dans les deux protocoles (BCJL et BCJL$_\delta$) et nous pouvons donc parler de ce résultat $\hat{x}$ sans ambiguïté.

Considérons maintenant le cas où $d(x, \hat{x}) > \delta n$, alors la probabilité que $x_i = \hat{x}_i$ pour tout $i \in T$ est au plus $2^{-\delta n}$. On peut en déduire que si Bob rejette l'ouverture dans le sous-protocole OUVERTURE$_\delta$ avec le résultat de mesure $\hat{x}$, alors il rejette l'ouverture dans le sous-protocole OUVERTURE avec le même résultat de mesure avec probabilité au moins $1 - 2^{-\delta n}$. Si p_0 est la probabilité que Bob accepte l'ouverture dans le protocole original et p_0^δ est la même probabilité pour le protocole modifié, on a que $p_0 \leq p_0^\delta + 2^{-\delta n}$. Puisque l'argument ci-dessus tient aussi pour les ouvertures à $b = 1$ avec les probabilités correspondantes p_1 et p_1^δ, on a

$$p_0 + p_1 \leq p_0^\delta + p_1^\delta + 2 \cdot 2^{-\delta n} \leq 1 + \epsilon + 2^{-\delta n+1} \quad .$$

□

La proposition suivante établit la sécurité du protocole BCJL$_\delta$ contre une Alice malhonnête non adaptée. Sa preuve est assez simple et se base sur la distance minimale du code correcteur pour montrer qu'un même état fixe du côté de Bob ne peut être une mise en gage à 0 et à 1 en même temps.

Proposition 3.4.1. *Pour tout $\delta > 0$, le protocole* BCJL$_\delta$ *est $2^{-d/2+\delta n+h(\delta)n}$-contraignant contre adversaires projectifs non adaptés.*

Démonstration. Soit $\rho_{\mathsf{B}} \in \mathcal{D}(\mathcal{H}_{\mathsf{B}})$ l'état quantique de Bob après la phase de mise en gage avec les informations classiques w, g et s envoyées à Bob. Soit $\mathbb{V}_{x,\theta}^\delta := \sum_{z \in B^\delta(x)} |z\rangle\langle z|_\theta$ la mesure projective correspondant à la vérification de Bob dans le protocole BCJL$_\delta$ lorsqu'Alice annonce (x, θ) pendant l'ouverture. Pour

toute paire d'ouvertures distinctes (x,θ) et (x',θ'),

$$\begin{aligned}\operatorname{tr}\left(\mathbb{V}^{\delta}_{x,\theta}\rho_B\right)+\operatorname{tr}\left(\mathbb{V}^{\delta}_{x',\theta'}\rho_B\right) &= \operatorname{tr}\left((\mathbb{V}^{\delta}_{x,\theta}+\mathbb{V}^{\delta}_{x',\theta'})\rho_B\right)\\ &\leq \left\|(\mathbb{V}^{\delta}_{x,\theta}+\mathbb{V}^{\delta}_{x',\theta'})\rho_B\right\|_1\\ &\leq \|\mathbb{V}^{\delta}_{x,\theta}+\mathbb{V}^{\delta}_{x',\theta'}\|_\infty\\ &\leq 1+\|\mathbb{V}^{\delta}_{x,\theta}\mathbb{V}^{\delta}_{x',\theta'}\|_\infty \ .\end{aligned}$$

où la première inégalité découle du fait que la norme de trace est monotone (inégalité (2.26)), la seconde inégalité par découle de la relation (2.25) et la dernière inégalité est une application du lemme 2.3.1.

On peut utiliser une technique provenant de [Sch07] pour borner la quantité $\|\mathbb{V}^{\delta}_{x,\theta}\mathbb{V}^{\delta}_{x',\theta'}\|_\infty$. Pour tout $|\psi\rangle$,

$$\begin{aligned}\left\|\mathbb{V}^{\delta}_{x,\theta}\mathbb{V}^{\delta}_{x',\theta'}|\psi\rangle\right\| &= \left\|\sum_z |z\rangle\langle z|_\theta \sum_{z'} |z'\rangle\langle z'|_{\theta'}|\psi\rangle\right\|\\ &\leq \left(\max_{\substack{z\in B^\delta(x)\\ z'\in B^\delta(x')}} |\langle z|_\theta|z'\rangle_{\theta'}|\right)\cdot\left\|\sum_z |z\rangle_\theta\right\|\cdot\left|\sum_{z'}\langle z'|_{\theta'}|\psi\rangle\right|\\ &\leq \left(\max_{\substack{z\in B^\delta(x)\\ z'\in B^\delta(x')}} |\langle z|_\theta|z'\rangle_{\theta'}|\right)\cdot\sqrt{|B^\delta(x)|}\cdot\sum_{z'}|\langle z'|_{\theta'}|\psi\rangle|\\ &\leq \left(\max_{\substack{z\in B^\delta(x)\\ z'\in B^\delta(x')}} |\langle z|_\theta|z'\rangle_{\theta'}|\right)\cdot\sqrt{|B^\delta(x)||B^\delta(x')|}\end{aligned}$$

où la deuxième inégalité ci-dessus est l'inégalité du triangle et les bornes en fonction de $|B^\delta(\cdot)|$ découlent de Cauchy-Schwartz. En utilisant le fait que $d(z,z')\geq d-2\delta n$ pour $z\in B^\delta(x)$ et $z'\in B^\delta(x')$ pour n'importe quelles chaines x et x' de syndrome s, et le fait que $|B^\delta(x)|\leq 2^{h(\delta)n}$, on obtient que $\|\mathbb{V}^{\delta}_{x,\theta}\mathbb{V}^{\delta}_{x',\theta'}\|_\infty \leq 2^{-d/2+\delta n+h(\delta)n}$ par la définition de la norme spectrale. En maximisant sur les ouvertures (x,θ) à 0 et les ouvertures (x',θ') à 1, on conclut que

$$P_0^{\mathrm{NA}}(\rho_{\mathsf{AB}})+P_1^{\mathrm{NA}}(\rho_{\mathsf{AB}}) = \max_{(x,\theta)}\operatorname{tr}\left(\mathbb{V}_{x,\theta}\rho_{\mathsf{B}}\right)+\max_{(x',\theta')}\operatorname{tr}\left(\mathbb{V}_{x',\theta'}\rho_{\mathsf{B}}\right)\leq 1+2^{-d/2+\delta n+h(\delta)n} \ . \qquad \square$$

Puisque le protocole de mise en gage BCJL_δ est non interactif, il découle directement du théorème 3.4.1 et de la proposition 3.4.1 que BCJL_δ est $2^{\frac{1}{2}(q-d/2+\delta n+h(\delta)n)}$-contraignant contre les adversaires projectifs q-bornés. En combinant ce fait avec le lemme 3.4.2, on obtient le résultat principal de cette sous-section établissant la sûreté du protocole BCJL contre un envoyeur malhonnête dans notre variante du modèle a mémoire bornée.

Théorème 3.4.3. *Pour tout $\delta>0$, le protocole de mise en gage* BCJL *est $(2^{\frac{1}{2}(q-d/2+\delta n+h(\delta)n)}+2\cdot 2^{-\delta n})$-contraignant contre adversaires projectifs q-bornés.*

3.5 Conclusion

Dans ce chapitre, nous avons considéré une situation fréquente en cryptographie où un adversaire contre un protocole détient de l'information auxiliaire corrélée (quantiquement) avec l'état du participant honnête. Le résultat principal de ce chapitre met en relation les attaques adaptées, où l'adversaire a accès à de l'information auxiliaire quantique, aux attaques non adaptées, où l'adversaire n'a pas accès à cette information auxiliaire. Cette relation A-vs-NA dit que l'avantage que confère cette information auxiliaire est limitée par une nouvelle mesure d'information, la max-information accessible, qui est elle-même bornée supérieurement par la taille — en qubits — de l'information auxiliaire.

Notre relation entre adversaires adaptés et non adaptés est l'outil principal pour montrer qu'un nouveau protocole de mise en gage dans le modèle $\mathcal{F}_{1\text{cc}}$-hybride est sûr. Ce protocole de mise en gage est par la suite utilisé pour établir la complétude de $\mathcal{F}_{1\text{cc}}$ dans le modèle UC, apportant ainsi une réponse à la principale question ouverte de [FKS+13].

La relation A-vs-NA est par la suite utilisée pour établir un résultat général sur la sécurité de protocoles quantiques de mise en gage. En particulier, notre relation permet de montrer que pour une famille générale de protocoles de mise en gage non interactifs, la sûreté contre les adversaires adaptés se réduit à la sûreté contre les adversaires non adaptés. Cette réduction peut être directement appliquée à un cas concret pour montrer que le protocole de mise en gage BCJL est sûr dans le modèle à mémoire bornée.

3.5.1 Problèmes ouverts

Dans la section 3.2.1, nous avons vu comment notre nouvelle mesure d'information, la *max-information accessible* $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_\rho$, peut être bornée supérieurement par la taille du registre A, calculée par sa max-entropie $\mathrm{H}_0(\mathsf{A})_\rho$. Un problème qui demeure non résolu est de borner supérieurement $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_\rho$ dans un modèle à mémoire *bruitée*. En particulier, nous avons tenté sans succès de borner supérieurement $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_\rho$ avec la condition générale présentée dans [KWW12] pour unifier les modèles de bruit. Cette condition quantifie le bruit en fonction du *taux* auquel peut être transmise de l'information classique par un état quantique qu'on soumet au bruit.

Un second problème ouvert concerne la deuxième partie de ce chapitre sur les protocoles de mise en gage non interactifs. Nous montrons une réduction des adversaires adaptés aux adversaires non adaptés pour ce type de protocole dans une version renforcée du modèle à mémoire bornée où les adversaires sont limités à des attaques qui utilisent des mesures projectives. Cette restriction est due à notre technique de preuve qui demande que ces mesures soient répétables, et la question qui demeure est de savoir si

cette restriction est nécessaire. Celle-ci pourrait être retirée soit en changeant de technique de preuve, permettant des attaques arbitraires de l'adversaire, soit en montrant que l'état ρ^0 défini au lemme 3.4.1 satisfait $\mathrm{I}_{\max}(\mathsf{B};\mathsf{A})_{\rho^0} \leq \mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho}$.

Notons finalement que si les deux questions ouvertes ci-dessus étaient résolues, alors les travaux de la seconde partie du chapitre 3 s'appliqueraient alors au modèle à mémoire bruitée, c'est-à-dire qu'un protocole de mise en gage non interactif qui est contraignant contre un adversaire non adapté l'est aussi contre un adversaire adapté dans le modèle à mémoire bruitée, pour un modèle de bruit qui nous permet de borner supérieurement $\mathrm{I}^{\mathrm{acc}}_{\max}(\mathsf{B};\mathsf{A})_{\rho}$.

La dernière question qui reste ouverte après les travaux de ce chapitre concerne la définition du critère contraignant des protocoles non interactifs (la définition 3.4.2). Cette définition est clairement plus forte qu'en général lorsqu'elle concerne les protocoles de mise en gage non interactifs pour les raisons énoncées à la fin de la sous-section 3.4.1. La question qui nous intéresse dans ce cas est de savoir s'il est possible de trouver une définition équivalente à la définition 3.4.2, mais qui est énoncée en termes de l'existence d'un bit (aléatoire) qu'il n'est pas possible de dévoiler, sauf avec probabilité négligeable. Une question semblable a été résolue dans [FF16], mais pour le cas général (c'est-à-dire pour les protocoles de mise en gage qui ne sont pas nécessairement non interactifs).

Chapitre 4

Échantillonnage quantique d'états mixtes

Ce chapitre porte sur la deuxième partie des travaux de cette thèse. Ces travaux ont été effectués en collaboration avec Frédéric Dupuis, Serge Fehr et Louis Salvail et ont été consignés dans un article [DFLS17] non publié au moment de l'écriture du présent document.

4.1 Introduction

4.1.1 Contexte et motivation

L'échantillonnage est une des tâches les plus fondamentales en statistique : elle permet de tirer des conclusions sur une grande population en regardant seulement un petit sous-ensemble de cette population. Par exemple, on peut estimer le nombre de zéros dans une chaine de n bits avec très grande précision en regardant seulement un petit sous-ensemble aléatoire de ces bits. C'est aussi vrai lorsque la population est *quantique* : étant donné un registre de n qubits, on peut déduire que son état est presque entièrement contenu dans un sous-espace de la forme $\text{span}\{|s\rangle : (\delta \pm \epsilon)n$ positions de s ont la valeur $1\}$ en mesurant un petit sous-ensemble des qubits dans la base calculatoire et en observant qu'une fraction δ des bits obtenus sont des 1 [BF10].

Une tâche qui est par contre impossible classiquement est de déduire par quelle distribution de probabilité une population a été générée par le simple échantillonnage statistique. Tandis que l'échantillonnage

peut nous dire qu'une chaine de n bits contient environ autant de zéros que de uns, on ne peut pas en conclure que ces bits furent générés par n lancés d'une pièce non biaisée ; rien n'exclut qu'il puisse s'agir d'une chaine fixe qui a la propriété d'avoir autant de zéros que de uns. Si cette tâche était possible, cela aurait des implications intéressantes pour la cryptographie : il serait possible, par exemple, d'obtenir un protocole pour le tirage d'une pièce (c'est-à-dire pour la primitive CT) en ayant un participant qui génère des bits uniformément distribués et en ayant l'autre participant qui vérifie que la plupart des bits reçus sont effectivement distribués selon le lancer d'une pièce non biaisée en utilisant cet échantillonnage hypothétique.

Bien que cette tâche soit clairement impossible dans le monde classique, il se trouve qu'elle a un sens dans le monde quantique. C'est dû au phénomène de purification : étant donné un état quantique mixte ρ_{A} sur un registre A (ce qui correspond à une distribution de probabilité sur les états purs), il est possible de définir un état biparti pur $|\psi\rangle_{\mathsf{AR}}$ sur un plus grand registre AR dont l'état réduit de A est ρ_{A}. Il est donc possible de s'assurer que A est dans l'état mixte ρ_{A} si on dispose du registre de purification R en vérifiant que les registres AR sont bien dans l'état $|\psi\rangle_{\mathsf{AR}}$ par une simple mesure projective. Pour donner un exemple plus concret, considérons un état ρ_{A} correspondant à un qubit uniformément distribué, c'est-à-dire $\rho_{\mathsf{A}} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. Alors, l'état pur $|\psi\rangle_{\mathsf{AR}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ purifie ρ_{A}, et il est donc possible de vérifier que ρ_{A} est uniformément distribué en s'assurant que l'état des registres combinés AR est $|\psi\rangle$. Notons aussi qu'il n'est pas nécessaire de faire confiance à la *source* des purifications, rendant cette idée applicable dans un contexte adversariel.

De la discussion ci-dessus découle un protocole d'échantillonnage naturel. Supposons qu'un *échantillonneur* Sam détient un état quantique arbitraire ρ_{A^n} de n sous-registres identiques A, préparés par un *prouveur* possiblement malhonnête Paul. Sam veut s'assurer que les registres qu'il détient sont dans un état près d'un *état de référence mixte* de la forme $\varphi^{\otimes n}$, avec possiblement quelques erreurs sur une petite quantité de positions. Pour ce faire, il choisit un échantillon aléatoire de k positions parmi les n et demande au prouveur Paul de lui fournir les registres de purification R^k pour ces positions. Il mesure ensuite chacun des systèmes conjoints AR échantillonnés avec la mesure projective $\{|\varphi\rangle\langle\varphi|_{\mathsf{AR}}, \mathbb{1} - |\varphi\rangle\langle\varphi|_{\mathsf{AR}}\}$ pour une certaine purification $|\varphi\rangle_{\mathsf{AR}}$ de φ_{A}. Il n'accepte le résultat de la vérification que si aucune erreur n'est détectée.

Il est important de préciser que pour l'échantillonnage d'un état mixte, une certaine forme d'interaction avec un prouveur *est nécessaire* puisque, comme le cas classique ne peut distinguer n lancers d'une pièce non biaisée d'une chaine contenant autant de 0 que de 1, aucune mesure locale du côté de l'échantillonneur ne peut distinguer l'état correct $\varphi^{\otimes n}$ d'un état composé des vecteurs propres de φ dans les bonnes proportions (c'est-à-dire selon les valeurs propres correspondantes).

4.1.2 Notre contribution

Dans la première partie de ce chapitre, nous étudions le type d'échantillonnage décrit ci-dessus en détail. Plusieurs défis surviennent lors de l'analyse du protocole. Premièrement, il n'est pas clair a priori comment définir formellement ce qu'on veut dire lorsqu'on dit que l'échantillonnage « fait son travail ». Dans le cas de l'échantillonnage quantique avec états de référence purs [BF10], on établit que l'état a une très faible probabilité de se trouver à l'extérieur d'un *sous-espace typique* qui correspond aux statistiques observées (voir par exemple le lemme 3.3.1 dans la section 3.3). Pour les états mixtes, cette définition échoue complètement. Par exemple, pour certifier l'état de référence uniformément distribué, cet espace typique correspond à l'espace de Hilbert en entier, ce qui mène à un énoncé trivial. On pourrait alors être tenté d'inclure le registre de purification dans cette définition du sous-espace typique, mais nous n'avons aucune garantie que l'adversaire respectera la structure que nous tentons d'imposer sur l'état — on ne sait même pas si son registre consiste en n sous-systèmes. Une seconde difficulté provient du fait que le prouveur ne fournira pas nécessairement l'état qui lui donne la meilleure chance de passer le test, même s'il le peut. Si on considère encore le cas des qubits uniformément distribués, même si Sam détient l'état idéal avant le début de l'échantillonnage, Paul peut essayer de biaiser le résultat de Sam, par exemple en réussissant le test s'il mesure $|0\rangle$ sur tous les qubits non échantillonnés et en échouant délibérément sinon. À cause de toutes ces difficultés, notre résultat d'échantillonnage ne suit pas du tout la même approche que les théorèmes d'échantillonnage traditionnels.

La seconde partie de ce chapitre est consacrée à appliquer notre résultat d'échantillonnage au tirage d'une pièce par le protocole qui découle naturellement du protocole d'échantillonnage décrit plus haut : un participant prépare plusieurs copies de la purification d'une pièce non biaisée quantique $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et l'autre participant vérifie la validité de l'état par l'échantillonnage. Considérant que la fonctionnalité idéale $\mathcal{F}_{\text{CT}}$ n'est pas réalisable sans hypothèse, il est naturel de se demander à quel point on peut s'en approcher. Cette question a été étudiée de fond en comble du point de vue du biais individuel de chaque lancer (voir la section 4.1.3 plus bas). Nous examinons cette question par une approche différente — et quelque peu orthogonale — où au lieu d'optimiser le biais des lancers individuels, on veut plutôt maximiser l'entropie globale des n bits de sortie. Nous montrons que le protocole de lancer de pièces évoqué ci-dessus permet à deux participants de produire une chaine de bit commune, où la min-entropie de cette chaine est une fraction arbitrairement grande de la min-entropie maximale (sauf avec probabilité négligeable). Classiquement, la quantité maximale d'incertitude qu'il est possible d'atteindre est $n/2$ bits de min-entropie, par le protocole naturel où chacun des participants pige $n/2$ bits au hasard et la sortie est la concaténation des bits de chacun [HMQU06].

4.1.3 Travaux précédents

Les résultats classique d'échantillonnage datent des travaux fondateurs de la théorie de la probabilité moderne de Bernstein, Hoeffding et Chernoff sur la concentration de la mesure dans les années 1920 et 1930. Plus récemment, plusieurs généralisations de ces résultats au monde quantique ont été prouvées. Ces généralisations incluent, par exemple, la borne de Chernoff sur les opérateurs de Ahlswede et Winter [AW02] et la borne de Chernoff quantique de [ACMT+07]. Toutefois, contrairement à leurs analogues classiques, ces généralisations s'appliquent difficilement à des résultats d'échantillonnage. D'autres résultats quantiques peuvent être utilisés pour analyser l'échantillonnage dans certains contextes tels les théorèmes de type *de Finetti* pour, par exemple, la distribution de clé quantique [Ren05, Ren07, CKR09a].

L'analogue quantique le plus direct des résultats d'échantillonnage classiques est certainement le théorème d'échantillonnage de [BF10]. Les auteurs y montrent une méthode générale pour transposer des résultats d'échantillonnage classiques au cas quantique. En gros, ils montrent que si un protocole d'échantillonnage classique permet de montrer qu'une chaine de variables aléatoires $X_1, \ldots, X_n$ appartient à un *bon* sous-ensemble $\mathcal{X}_{\text{bon}}$ avec très grande probabilité, alors la version quantique du même protocole d'échantillonnage (défini précisément dans [BF10]) permet de dire qu'un état $\rho_{X_1,\ldots,X_n}$ est presque entièrement contenu dans le *bon* sous-espace $\text{span}\{|x_1\rangle \otimes \cdots \otimes |x_n\rangle : x_1, \ldots, x_n \in \mathcal{X}_{\text{bon}}\}$. Ce *bon* ensemble correspond normalement aux chaines qui sont compatibles avec les observations de l'échantillon. Notre résultat d'échantillonnage peut être interprété comme une extension du résultat ci-dessus au cas de l'échantillonnage d'états mixtes.

L'application principale de notre résultat d'échantillonnage, le tirage d'une pièce, a aussi un long historique. La tâche en soi fut introduite par Manuel Blum [Blu82] en 1981. Depuis le début des années 2000, cette tâche a reçu beaucoup d'attention de la part de la communauté cryptographique quantique puisque c'est une des tâches les plus naturelles pour lesquelles la mécanique quantique permet quelque chose d'impossible classiquement. Il existe deux versions du tirage d'une pièce : le tirage *fort* où le protocole doit être équivalent à une boîte noire qui produit un bit uniformément distribué et le tirage *faible* où chaque participant a un résultat de prédilection connu par l'autre et où aucun des deux ne peut biaiser la sortie du protocole vers son résultat. Plusieurs protocoles quantiques pour le tirage fort furent développés avec divers biais [SR01, Amb04], mais une borne inférieure fondamentale de $(\frac{1}{\sqrt{2}} - \frac{1}{2})$ sur le biais de tels protocoles fut prouvé dans [Kit03] (voir aussi [GW07]). Finalement, un protocole avec un biais optimal fut prouvé dans [CK09]. Pour le tirage faible, plusieurs protocoles avec divers biais ont aussi été proposés [KN04, SR02, Moc04, Moc05], mais culminants cette fois avec un protocole dont le biais est arbitrairement petit [Moc07]. Le tirage à pile ou face quantique a également été implémenté en laboratoire [PJL+14]. Dans ce chapitre, nous allons dans une direction quelque peu orthogonale aux résultats

susmentionnés : malgré le fait que le tirage fort avec biais négligeable est impossible, nous montrons que le biais peut disparaitre asymptotiquement lorsqu'on tire plusieurs pièces. Plus précisément, on montre que deux participants peuvent produire une chaine commune de min-entropie arbitrairement près du maximum, sauf avec probabilité négligeable.

Un protocole similaire à celui décrit dans la section 4.5 a été proposé par Salvail et Høyer en 1999 [HS99] qui atteint le même biais que [Amb01] pour le tirage fort, c'est-à-dire un biais de $\frac{1}{4}$. Dans ce protocole, Alice prépare deux paires EPR et envoie la moitié de chacune à Bob. Bob choisit un des deux qubits au hasard et vérifie qu'Alice détient le registre de purification correspondant en lui demandant le résultat de la mesure de ce registre dans une base aléatoirement choisie avant de comparer ce résultat avec celui de sa propre mesure dans la même base. Si les deux résultats sont identiques, cela donne à Bob une certaine confiance sur le fait que la paire restante peut être utilisée comme un tirage à pile ou face. Ce protocole peut être vu comme un cas particulier de notre protocole avec une population de taille $n = 2$ et un échantillon de taille $k = 1$. Augmenter la taille de la population et de l'échantillon augmente la confiance que Bob a dans le fait que les paires restantes sont *près* de tirages à piles ou face idéaux.

4.2 Échantillonnage d'une population quantique avec état de référence *mixte*

La tâche que nous cherchons à analyser peut être modélisée comme un *jeu* entre deux participants : un *prouveur* Paul et un *échantillonneur* Sam. Paul doit préparer plusieurs copies d'un *état de référence* φ et les envoyer à Sam. Le but de ce jeu pour Sam est de détecter si l'état envoyé par Paul est (près de) l'état prescrit, peu importe la stratégie de Paul qui peut vouloir tricher à ce jeu. L'état de référence φ peut être une matrice de densité arbitraire, mais connue, vivant dans un espace de Hilbert de dimension finie.

Pour se convaincre que l'état envoyé par Paul est de la bonne forme, Sam demande à Paul de prendre part à un *protocole d'échantillonnage quantique* qui décrit comment Paul doit préparer l'état et comment Sam en fera la vérification. Un example d'un tel protocole est illustré à la figure 4.1 où Sam demande à Paul de préparer N purifications de φ et de garder les registres de purification de chaque position. La vérification de Sam consiste à demander un sous-ensemble aléatoire de k de ces registres de purification et de s'assurer qu'ils purifient bien l'état de ses registres correspondants. Notons qu'il n'y a pas de perte de généralité à annoncer à Paul les k positions vérifiées *d'un seul coup* comme il est fait dans le protocole de la figure 4.1 : annoncer ces positions *une à une* ne fait que compliquer la tâche du prouveur car un adversaire qui apprend l'ensemble des positions échantillonnées peut simuler un adversaire qui l'apprend

position par position. Ainsi notre analyse s'applique également pour le cas séquentiel.

Protocole d'échantillonnage par purification

Paramètres : $N \in \mathbb{N}$, $\beta \in \mathbb{R}$ tel que $0 < \beta < 1$ et $\varphi \in \mathcal{D}(\mathcal{H}_{\mathsf{S}})$.

1. Paul prépare N copies de la purification $|\varphi_{\mathsf{PS}}\rangle$ de φ_{S}. Il envoie les N copies du registre S étiquetés S_1 to S_N à Sam et garde les registres de purification P_1 à P_N correspondants.
2. Sam choisit aléatoirement un sous-ensemble $t \subseteq [N]$ de taille $k = \lceil \beta N \rceil$.
3. Sam envoie t à Paul et lui demande le registre de purification P_i pour chaque $i \in t$.
4. Sam mesure chacun des registres conjoints $\mathsf{P}_i\mathsf{S}_i$ pour $i \in t$ avec la mesure projective $\{|\varphi\rangle\langle\varphi|_{\mathsf{PS}}, \mathbb{1}_{\mathsf{PS}} - |\varphi\rangle\langle\varphi|_{\mathsf{PS}}\}$. Sam accepte s'il obtient le résultat $|\varphi\rangle\langle\varphi|^{\otimes k}$, sinon, il rejette.

FIGURE 4.1 – Le protocole d'échantillonnage par purification avec état de référence φ_{S} et purification $|\varphi_{\mathsf{PS}}\rangle$ de φ_{S}.

Dans le cas extrême d'un état de référence *pur*, et donc pour lequel il n'y a pas de purification du côté de Paul, le protocole d'échantillonnage de la figure 4.1 coïncide avec le protocole présenté et analysé dans [BF10] pour la stratégie d'échantillonnage classique qui correspond à choisir un échantillon uniforme de k positions (voir section 4.2.1 plus bas). Pour un état réellement mixte, par contre, il est beaucoup plus difficile de montrer que le protocole de la figure 4.1 « fait son travail ». La principale difficulté se trouve dans les degrés de liberté additionnels donnés à Paul dans la préparation des purifications d'une manière qui peut dépendre du choix de l'échantillon $t \subset [N]$. Ceci rend les techniques de [BF10] inapplicables. En effet, l'intuition derrière l'analyse de [BF10] est de supposer, pour les besoins du raisonnement, que les positions à l'extérieur de l'échantillon t sont également mesurées. Le choix de t peut alors être repoussé après la mesure, puisque toutes les positions sont mesurées, et ainsi on peut se réduire à un échantillonnage classique sur le résultat de la mesure. Dans notre cas, puisque le choix des purifications de Paul dépend de t, nous ne pouvons pas parler du résultat de la mesure *avant* le choix de t ou même de cette mesure sur les positions *à l'extérieur* de t. Puisque, comme brièvement mentionné dans l'introduction, tout protocole conçu pour échantillonner des états mixtes requiert une certaine forme d'interaction avec un prouveur, il est clair que nous avons besoin d'une approche différente pour analyser de tels protocoles, en particulier celui de la figure 4.1.

Avant d'analyser le protocole d'échantillonnage de la figure 4.1, on doit d'abord préciser ce à quoi on s'attend de la sortie d'un tel protocole d'échantillonnage. On veut qu'après le protocole, l'état des registres restants de Sam soit *près* de l'état idéal $\varphi^{\otimes n}$ où $n = N - k$, mais ce n'est pas totalement évident comment définir une notion de proximité qui soit à la fois non triviale et prouvable dans notre contexte.

Il est utile de commencer par regarder le type d'attaque que Paul peut monter avec une probabilité non négligeable de passer le test de Sam. Clairement, Paul peut dévier du comportement honnête pour une petite quantité de positions sans se faire prendre. Autrement dit, il peut préparer un état consistant de N copies de $|\varphi\rangle$, mais en modifiant un petit nombre de positions de manière arbitraire, et passer le test avec bonne probabilité. Évidemment, Paul peut aussi tricher en préparant une mixture de tels états et, par la purification, avec aussi une superposition de tels états. Ceci motive la définition suivante d'*état idéal*, qui capture essentiellement le meilleur qu'on puisse espérer pour l'état post-échantillonnage de Sam. L'énoncé formel de ce que le protocole de la figure 4.1 accomplit viendra apparenter l'état post-échantillonnage de Sam à un état idéal tel que défini ci-dessous. Cette approche est comparable à l'approche de [BF10] pour les états purs où on apparente l'état réel à un état idéal, bien qu'il subsiste des différences techniques.

Définition 4.2.1 (État idéal)**.** Pour $\epsilon > 0$, un état $\psi_{\mathsf{S}^n} \in \mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{S}}^{\otimes n})$ est ϵ-*idéal* s'il existe une purification $|\psi_{\mathsf{R}\mathsf{P}^n\mathsf{S}^n}\rangle$ de ψ_{S^n} telle que

$$|\psi\rangle_{\mathsf{R}\mathsf{P}^n\mathsf{S}^n} \in \mathcal{H}_{\mathsf{R}} \otimes \Delta_{\epsilon n}(|\varphi\rangle_{\mathsf{P}^n\mathsf{S}^n}^{\otimes n}) \ . \tag{4.1}$$

où $\Delta_{\epsilon n}$ représente la sphère de Hamming quantique (définition 2.9.1). On dit que l'état ψ_{S^n} est *idéal* s'il est ϵ-idéal.

Notre analyse du protocole décrit dans la figure 4.1 préserve plusieurs des aspects de l'interprétation opérationnelle des résultats de [BF10] pour le cas de l'échantillonnage d'états purs. Notre résultat permet de montrer que l'état résiduel de Sam peut être considéré comme étant idéal dans de nombreuses situations. Plus formellement, notre résultat principal (théorème 4.4.1 et le corollaire 4.4.2) montre que l'état *sous-normalisé*[1] de Sam après le protocole d'échantillonnage est borné supérieurement par un opérateur (presque) idéal. Soit $d := \dim(\mathcal{H}_{\mathsf{S}})$ la dimension de l'espace de Hilbert auquel appartient φ_{S} et soit $\epsilon > 0$. Informellement, notre résultat d'échantillonnage dit que l'état sous-normalisé de Sam après l'échantillonnage $\rho_{\mathsf{S}^n}^{\text{acc}} \in \mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{S}}^{\otimes n})$ satisfait

$$\rho_{\mathsf{S}^n}^{\text{acc}} \leq (N+1)^{d^2-1}\psi_{\mathsf{S}^n} + \sigma_{\mathsf{S}^n} \ , \tag{4.2}$$

où ψ_{S^n} est idéal et où $\|\sigma_{\mathsf{S}^n}\|_1$ est négligeable en N.

N'importe quel état $\rho_{\mathsf{S}^n}^{\text{acc}}$ qui satisfait (4.2) peut être considéré comme un état idéal dans plusieurs applications. Soit $\mathcal{Q}$ un superopérateur complètement positif qui n'augmente pas la trace (un CPTN) représentant une tâche qu'on veut appliquer sur $\rho_{\mathsf{S}^n}^{\text{acc}}$. Supposons que $\mathcal{Q}$ se comporte « bien » lorsqu'exécuté sur l'état idéal ψ_{S^n} de (4.2), c'est-à-dire qu'un « mauvais » évènement représenté par un élément de POVM

1. L'état sous-normalisé de Sam après le protocole d'échantillonnage est l'état conditionné sur le fait qu'il accepte le test, pondéré par la probabilité qu'il accepte ce test. L'utilisation d'un état sous-normalisé plutôt que normalisé n'est qu'une considération esthétique pour simplifier l'expression (4.2) en faisant abstraction de la probabilité de passer le test.

$0 \leq E \leq \mathbb{1}$ a probabilité négligeable de survenir sur l'état idéal :

$$p^{\text{id}} := \text{tr}\left(E \cdot \mathcal{Q}(\psi_{\mathsf{S}^n})\right) \leq 2^{-\alpha N}$$

pour $\alpha > 0$. Exécuter $\mathcal{Q}$ sur $\rho_{\mathsf{S}^n}^{\text{acc}}$ produit un état qui satisfait $\mathcal{Q}(\rho_{\mathsf{S}^n}^{\text{acc}}) \leq \mathcal{Q}((N+1)^{d^2-1}\psi_{\mathsf{S}^n} + \sigma_{\mathsf{S}^n})$ en utilisant (4.2) et le fait que $\mathcal{Q}$ est complètement positif. On a alors que la probabilité du « mauvais » évènement sur cet état *réel* est

$$p^{\text{réel}} := \text{tr}\left(E \cdot \mathcal{Q}(\rho_{\mathsf{S}^n}^{\text{acc}})\right) \leq (N+1)^{d^2-1} p^{\text{id}} + \|\sigma_{\mathsf{S}^n}\|_1$$

qui reste négligeable en N. Autrement dit, n'importe quel processus quantique aboutissant à un « mauvais » résultat sur un état idéal avec probabilité négligeable a aussi probabilité négligeable d'aboutir à un « mauvais » résultat lorsqu'appliqué sur l'état post-échantillonnage (réel). Ainsi, il est suffisant d'analyser la probabilité de ce « mauvais » évènement sur l'état idéal, ce qui est normalement plus facile grâce à la forme spécifique de cet état donnée par (4.1).

Notons aussi que si on veut une interprétation de notre résultat principal en terme d'état *conjoint* de Paul et Sam, nous pouvons évoquer la proposition 2.9.1 sur (4.2). Pour simplifier la notation, supposons que $\rho_{\mathsf{S}^n}^{\text{acc}} \leq c \cdot \psi_{\mathsf{S}^n}$, où $c := (N+1)^{d^2-1}$. La proposition 2.9.1 nous dit alors qu'il existe un opérateur linéaire V agissant sur les registres RP^n tel que $V^*V \leq \mathbb{1}_{\mathsf{RP}^n}$ et tel que

$$|\rho^{\text{acc}}\rangle_{\mathsf{RP}^n\mathsf{S}^n} = \sqrt{c}(V_{\mathsf{RP}^n} \otimes \mathbb{1}_{\mathsf{S}^n})|\psi\rangle_{\mathsf{RP}^n\mathsf{S}^n} \quad , \tag{4.3}$$

où $|\rho^{\text{acc}}\rangle_{\mathsf{RP}^n\mathsf{S}^n}$ et $|\psi\rangle_{\mathsf{RP}^n\mathsf{S}^n}$ sont des purifications de $\rho_{\mathsf{S}^n}^{\text{acc}}$ et ψ_{S^n}, respectivement. L'opérateur V peut être perçu comme un élément $V = M_0$ appartenant à une mesure non destructive $\{M_a\}_a$ appliquée sur les registres RP^n et l'état (4.3) peut être perçu comme l'état conditionné sur le résultat $a = 0$ de cette mesure, pondéré par le facteur $\sqrt{c}$. On peut en conclure que si la probabilité que Paul puisse produire un « mauvais » état conjoint à partir de l'état idéal est négligeable, alors la probabilité qu'il puisse produire un tel état à partir de l'état réel est aussi négligeable.

4.2.1 Cas spécial : échantillonnage avec état de référence pur

Comme notre résultat d'échantillonnage concerne les états de référence mixtes, et comme les états purs sont un cas spécial des états mixtes, une question naturelle à se poser est de savoir si les résultats précédents sur l'échantillonnage quantique surviennent naturellement comme cas spéciaux de notre analyse. Dans cette sous-section, nous montrons comment une partie des résultats de [BF10], qui servent à montrer que les qubits non échantillonnés contiennent peu d'erreur si aucune erreur n'a été observée dans l'échantillon, découle directement de notre analyse des protocoles d'échantillonnage des états mixtes.

Le résultat d'échantillonnage de [BF10] dit essentiellement que si on mesure un sous-ensemble aléatoire de k sous-registres de S^N dans la base calculatoire [2] et qu'on obtient le résultat $|0\rangle^{\otimes k}$ (ce qui correspond au protocole de la figure 4.1 avec état de référence pur), alors l'état des sous-registres restants est dans la sphère de hamming quantique $\Delta^{\delta n}(|0\rangle^{\otimes n})$. Voyons comment nous pouvons recréer ce résultat à l'aide du nôtre.

Puisque dans le cas des états pur, il n'existe pas de registre de purification du côté d'un prouveur, la définition d'état idéal (définition 4.2.1) concerne seulement le registre de l'échantillonneur. Ainsi, notre résultat principal (corollaire 4.4.2) dit qu'il exite un état ψ_{S^n} qui a support dans $\Delta^{\delta n}(|0\rangle_{\mathsf{S}^n}^{\otimes n})$ tel que

$$\rho_{\mathsf{S}^n}^{\text{acc}} \leq (N+1)^{d^2-1}\psi_{\mathsf{S}^n} + \sigma_{\mathsf{S}^n} \tag{4.4}$$

où σ_{S^n} correspond à la partie de l'état qui échoue l'échantillonnage, et qui a donc une norme négligeable. Puisque le sous-espace $\Delta^{\delta n}(|0\rangle_{\mathsf{S}^n}^{\otimes n})$ est défini seulement sur le registre S^n, on peut projetter l'état résiduel de l'échantillonneur sur ce sous-espace. L'inégalité (4.4) implique alors que

$$\operatorname{tr}\left((\mathbb{1}_{\mathsf{S}^n} - \mathbb{P}_{\mathsf{S}^n}^{\delta n,|0\rangle})\rho_{\mathsf{S}^n}^{\text{acc}}\right) \leq (N+1)^{d^2-1}\operatorname{tr}\left((\mathbb{1}_{\mathsf{S}^n} - \mathbb{P}_{\mathsf{S}^n}^{\delta n,|0\rangle})\psi_{\mathsf{S}^n}\right) + \operatorname{tr}(\sigma_{\mathsf{S}^n}) = \operatorname{tr}(\sigma_{\mathsf{S}^n})$$

où $\mathbb{P}_{\mathsf{S}^n}^{\delta n,|0\rangle}$ est le projecteur sur le sous-espace $\Delta^{\delta n}(|0\rangle_{\mathsf{S}^n}^{\otimes n})$. Donc la probabilité d'échec de l'échantillonnage correspond à la trace de σ_{S^n}, qui est négligeable en N. En renormalisant ρ^{acc}, on obtient un énoncé non trivial sur l'état post-échantillonnage pourvu que la probabilité d'accepter l'issue de l'échantillonnage soit non négligeable.

On a ainsi montré que si l'échantillonneur observe l'état $|0\rangle^{\otimes k}$ aux positions échantillonnées, alors l'état post-échantillonnage est dans le sous-espace à peu d'erreurs $\Delta^{\delta n}(|0\rangle^{\otimes n})$, sauf avec probabilité négligeable. Nous retrouvons donc un résultat identique à celui de [BF10] pour l'état de sortie du protocole d'échantillonnage présenté plus haut. La seule différence réside dans la probabilité d'échec de l'échantillonnage (c'est-à-dire la probabilité que l'état de sortie se trouve à l'extérieur de $\Delta^{\delta n}(|0\rangle^{\otimes n})$).

4.3 Protocoles d'échantillonnage d'états mixtes

Dans cette section, nous présentons en plus de détails le type de protocole d'échantillonnage que nous analyserons dans la section 4.4. La propriété clé du protocole d'échantillonnage de la figure 4.1 qui fait en sorte que les techniques de la section 4.4 soient applicables est que ce protocole est invariant sous la permutation du registre de l'échantillonneur, avec un ajustement de l'attaque de l'adversaire et de l'état

2. Comme spécifié dans [BF10], lorsqu'on échantillonne des états de référence *purs*, il n'y a pas de perte de généralité à supposer que l'état de référence est l'état $|0\rangle$ dans une base fixe, car tout autre état peut être transformé en $|0\rangle$ par une transformation unitaire *locale* chez l'échantillonneur.

de sortie dépendant de cette permutation. Cette propriété peut se généraliser à n'importe quel protocole similaire à celui de la figure 4.1, ce qui motive la forme générale de protocole d'échantillonnage donnée par la figure 4.2. En cernant précisément les propriétés nécessaires à l'application de nos techniques de la section 4.4 par la définition 4.3.1, on obtient ainsi un critère suffisant pour l'analyse de protocoles de la forme de la figure 4.2.

Protocole général d'échantillonnage d'états mixtes

Paramètres : $N \in \mathbb{N}$, $\beta \in \mathbb{R}$ tel que $0 < \beta < 1$ et $\varphi \in \mathcal{D}(\mathcal{H}_{\mathsf{S}})$.

1. Paul prépare un état $\rho_{\mathsf{RS}^N} \in \mathcal{D}(\mathcal{H}_{\mathsf{R}} \otimes \mathcal{H}_{\mathsf{S}}^{\otimes N})$ et envoie le registre S^N à Sam.
2. Sam choisit un échantillon aléatoire $t \subset_R [N]$ de taille $k = \lceil \beta N \rceil$ et un défi c, et envoie t et c à Paul.
3. À la réception de t et c, Paul répond par un registre quantique Q.
4. Sam effectue une mesure à résultat binaire qui dépend de c et t sur le système composé des registres Q et S_i pour $i \in t$, et accepte ou rejette selon le résultat de cette mesure.

FIGURE 4.2 – La forme générale d'un protocole d'échantillonnage quantique avec état de référence mixte.

La forme générale des protocoles d'échantillonnage que nous considérons est donnée à la figure 4.2. Le protocole a comme paramètres de sécurité $N \in \mathbb{N}$ la taille de la population et $0 < \beta < 1$ qui détermine la taille de l'échantillon. Notons qu'avec paramètres N et β fixes, la sortie du protocole d'échantillonnage est toujours de taille $n = N - \lceil \beta N \rceil$, c'est-à-dire que l'état de sortie vit dans l'espace de Hilbert $\mathcal{H}_{\mathsf{S}}^{\otimes n}$. Une conséquence de ce choix est qu'il n'y a pas de liberté dans la manière dont on choisit t ; la seule distribution de probabilité sur les sous-ensembles de $[N]$ de taille $\lceil \beta N \rceil$ qui est invariante sous la permutation des positions est la distribution uniforme sur les sous-ensembles de cette taille.

Le message c que Sam envoie à Paul représente un *défi* ou une *question* que Sam pose à Paul en plus de l'échantillon t. Bien que son utilité ne soit pas évidente pour l'instant, nous verrons à la section 4.3.2 un exemple de protocole où la présence d'un tel c permet de remplacer la transmission du registre de purification par la transmission d'information classique.

L'instanciation évidente de ce protocole général est le protocole d'échantillonnage décrit par la figure 4.1, où c est vide et la mesure de Sam consiste en une mesure projective sur $|\varphi\rangle\langle\varphi|^{\otimes k}$. D'autres exemples sont donnés à la section 4.3.2, en particulier un protocole pour certifier des demi-paires EPR où le défi c correspond à la description d'une mesure que le prouveur doit effectuer sur ses registres de purification.

Étant donné un protocole de la forme donnée par la figure 4.2, l'attaque de l'adversaire est caractérisée par le choix de l'état initial ρ_{RS^N} et de l'opération quantique (qui dépend de t et de c) qui produit le registre Q à l'étape 3.

4.3.1 Invariance sous les permutations des protocoles d'échantillonnage

Nous présentons maintenant la notion d'invariance sous les permutations que doivent satisfaire les protocoles de la forme générale donnée par la figure 4.2 pour que notre résultat principal permette d'en analyser l'état de sortie. Cette notion diffère des définitions précédentes d'invariance sous les permutations d'états ou de super-opérateurs [CKR09b, Ren10], en particulier par la dépendance que l'attaque de l'adversaire peut avoir sur l'ordre des éléments. Cela fait en sorte que les techniques existantes exploitant les puissants outils qui viennent avec l'invariance sous les permutations, comme les théorèmes de style *de Finetti* et les résultats de *post-sélection*, ne sont pas directement applicables dans notre cas.

La notion d'invariance sous les permutations que nous considérons est donnée à la définition 4.3.1. Cette définition comprend également les autres hypothèses sur le protocole d'échantillonnage qui sont suffisantes pour pouvoir appliquer notre résultat principal. Intuitivement, on demande d'un protocole d'échantillonnage qu'il ne dépende pas de l'ordre des éléments et qu'il fonctionne bien sur un état « facile », c'est-à-dire un état de la forme $|\theta\rangle\langle\theta|^{\otimes N}$.

Définition 4.3.1 (Invariance sous les permutations pour les protocoles d'échantillonnage)**.** Un protocole d'échantillonnage qui implémente le modèle de la figure 4.2 est *invariant sous la permutation du registre de l'échantillonneur* si, pour toute stratégie adversarielle pour Paul, le CPTN $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$, qui représente la sortie du protocole d'échantillonnage, satisfait

1. pour tout état initial $\rho_{\mathsf{RS}^N} \in \mathcal{D}(\mathcal{H}_{\mathsf{R}} \otimes \mathcal{H}_{\mathsf{S}}^{\otimes N})$ il existe un CPTN $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ tel que

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} |\pi\rangle\langle\pi|_\Pi \otimes \pi_{\mathsf{S}^n}\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N})\pi^*_{\mathsf{S}^n} = \bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}) \tag{4.5}$$

   pour une purification symétrique $|\bar{\rho}\rangle_{\mathsf{P}^N\mathsf{S}^N} \in \text{Sym}^N(\mathcal{H}_{\mathsf{P}} \otimes \mathcal{H}_{\mathsf{S}})$ de $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N} \pi_{\mathsf{S}^N}\rho_{\mathsf{S}^N}\pi^*_{\mathsf{S}^N}$,

2. pour tout $\epsilon > 0$, si $F(\theta_{\mathsf{S}}, \varphi_{\mathsf{S}})^2 < 1 - \epsilon$, alors

$$\|\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}})\|_1 \leq \text{negl}(N)$$

   pour toute purification $|\theta\rangle_{\mathsf{PS}}$ de θ_{S},

3. et $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ satisfait la relation

$$\text{tr}_\Pi\left(\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}})\right) \leq \theta^{\otimes n}_{\mathsf{S}} \quad . \tag{4.6}$$

Examinons un par un les points de cette définition. Le premier critère demande que toute attaque contre le protocole d'échantillonnage pour un état initial ρ_{RS^N} puisse être transformée en une attaque *équivalente* où l'état initial est plutôt une purification de l'état de S^N auquel on applique une permutation aléatoire. Plus précisément, ce critère équivaut à dire que si Sam permutait ses registres avec une permutation aléatoire π qu'il annonce ensuite à Paul, ce dernier pourrait ajuster ses actions en fonction de π pour donner le même état de sortie, mais permuté en fonction de π. La raison pour laquelle nous supposons que l'état initial $\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}$ est dans le sous-espace symétrique est parce qu'il est possible pour l'adversaire de simuler le choix et l'annonce de π à partir du registre P^N d'un tel état.

Le second critère demande au protocole d'échantillonnage de rejeter avec très grande probabilité un état qui est i.i.d. en un état θ_{S} trop loin de φ_{S}. Intuitivement, les états de ce type sont les plus faciles à analyser pour l'échantillonnage. Leur indépendance limite sévèrement les attaques possibles d'un adversaire qui détient le registre de purification et le fait que chacun des états est « loin » de l'état de référence φ fait en sorte qu'une erreur a de fortes chances d'être détectée.

Finalement, le troisième critère demande au protocole d'échantillonnage de ne pas perturber l'état des registres qui ne sont pas échantillonnés, autre que par un réarrangement par la permutation appliquée sur le registre de sortie S^n. Cette propriété est essentiellement capturée par l'équation (4.6) pour les fins de la preuve : l'état de sortie est borné supérieurement par l'état d'entrée, à une permutation près. Bien que ce soit un critère naturel pour un protocole d'échantillonnage, capturé par le super-opérateur $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$, ce troisième point s'assure que $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ satisfait aussi cette propriété nécessaire pour les preuves de la section 4.4.

D'un point de vue technique, le premier critère nous permet d'appliquer les outils présentés à la section 2.8 sur l'état symétrique $\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}$ pour le borner supérieurement par une mixture d'états i.i.d. de la forme $\int |\theta\rangle\langle\theta|^{\otimes N} d|\theta\rangle$, et le deuxième critère nous permet de contrôler quelle partie de cette mixture survit au protocole d'échantillonnage. Ce qu'il reste à faire, et qui est étonnamment assez complexe, est de se débarrasser de la permutation sur le registre de sortie de l'échantillonneur et d'obtenir une borne supérieure sur l'état $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{RS^N})$ plutôt que sur sa version permutée. Les détails se trouvent dans la section 4.4.

Une manière plus « paresseuse » de gérer cette permutation aléatoire aurait été de simplement modifier le protocole d'échantillonnage pour *vraiment* permuter l'état de sortie du protocole de manière à ce que l'état final soit *égal* à la partie gauche de (4.5). À part être moins élégante comme solution, puisqu'elle mènerait à un protocole d'échantillonnage moins naturel et plus compliqué que nécessaire, cette modification donnerait également plus de puissance au participant qui choisit cette permutation, par la possibilité de la choisir de manière *adversarielle*. Par exemple, dans notre application sur le tirage à pile ou face de

la section 4.5, où l'état final est utilisé pour produire une source de haute min-entropie, on ne peut pas permettre à l'un ou l'autre des participants de permuter la sortie et, par exemple, bouger tous les zéros aux positions qu'il désire.

4.3.2 Exemples de protocoles d'échantillonnage

Dans cette sous-section, nous présentons quelques exemples de protocoles d'échantillonnages qui implémentent la forme générale donnée par la figure 4.2. Nous avons déjà vu l'un de ces protocoles à la figure 4.1 de la section précédente. Nous présentons aussi plus bas un protocole d'échantillonnage servant à certifier un type d'état bien précis, une demi-paire EPR, qui correspond à l'état de référence $\varphi = \frac{\mathbb{1}}{2}$.

Bien qu'il ne soit pas très difficile de montrer que les protocoles présentés dans cette section satisfont la définition 4.3.1, les preuves sont tout de même fastidieuses. Pour cette raison, nous présentons seulement l'intuition derrière chacune des preuves dans cette section. Les preuves complètes peuvent être trouvées à l'appendice A.

Protocole d'échantillonnage par purification

Le protocole d'échantillonnage par purification est celui que nous avons vu à la section 4.2, et est présenté à la figure 4.1. Ce protocole demande au prouveur de préparer N paires de registres PS dont l'état est une purification de l'état de référence φ_{S}. Paul envoie les N registres S à Sam et ce dernier, pour vérifier que ces registres sont bien dans l'état φ_{S}, demande à Paul de lui fournir les registres de purification P pour un sous-ensemble aléatoirement choisit de k positions parmi les N. Pour ce protocole, le défi c est vide. Sam vérifie ensuite que les k systèmes conjoints PS sont dans l'état $|\varphi\rangle_{\mathsf{PS}}$ pour une certaine purification $|\varphi\rangle_{\mathsf{PS}}$ de φ_{S} connue par Paul.

La preuve complète de la proposition 4.3.1 se trouve à l'appendice A.1.

Proposition 4.3.1. *Le protocole d'échantillonnage par purification (présenté à la figure 4.1) satisfait la définition 4.3.1.*

Ébauche de preuve. Pour le premier critère, il faut montrer que pour tout adversaire contre le vrai protocole, il existe un adversaire équivalent sur une version symétrique du protocole qui donnera le même état de sortie, à une permutation près. À partir d'une purification de $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N} \pi_{\mathsf{S}^N}\rho_{\mathsf{S}^N}\pi^*_{\mathsf{S}^N}$, Paul peut produire la permutation π qui est appliquée sur le registre S^N et ainsi savoir, lorsque Sam lui demande les registres de purification pour un échantillon t, comment ajuster son attaque par rapport à π. Dans sa

réponse, Paul doit aussi permuter les registres de purifications P pour qu'ils s'alignent comme il faut avec les bons registres S du côté de Sam. Cette attaque sur le protocole symétrique est équivalente à l'attaque de Paul sur le protocole régulier, à une permutation près sur les registres de sortie.

Le deuxième critère découle du fait que si l'état initial est i.i.d. en $|\theta\rangle\langle\theta|_{\mathsf{PS}}$, alors la probabilité maximale de passer le test est de transformer chacun des $|\theta\rangle_{\mathsf{PS}}$ en agissant sur P de manière à maximiser le produit interne avec $|\varphi\rangle_{\mathsf{PS}}$. Ce produit interne ne peut jamais excéder la fidélité entre θ_{S} et φ_{S} par le théorème d'Uhlmann, donc chaque position a probabilité au moins $\epsilon > 0$ d'échouer le test. Si Sam teste k positions, alors la probabilité de passer tous les tests est négligeable en k.

Le troisième critère découle facilement de la description de l'adversaire symétrique. □

Protocole d'échantillonnage à mesures locales de demi-paires EPR

Le protocole d'échantillonnage que nous présentons maintenant montre qu'il n'est pas toujours nécessaire au prouveur de fournir les registres de purification de chacune des positions échantillonnées pour que l'échantillonneur puisse tirer une conclusion sur l'état des registres non échantillonnés. Nous présentons à la figure 4.3 un protocole pour échantillonner des états de références de la forme $\varphi = \frac{\mathbb{1}}{2}$ (ce qui correspond à la moitié d'une paire EPR $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$) qui utilise seulement des *opérations locales de la communication classique* (OLCC). La proposition 4.3.2 établit que ce protocole satisfait la définition 4.3.1, ce qui implique qu'on peut utiliser les techniques de la section 4.4 pour montrer qu'il fonctionne comme voulu. La preuve complète de cette proposition peut être trouvée à l'appendice A.

Proposition 4.3.2. *Le protocole d'échantillonnage de la figure 4.3 satisfait la définition 4.3.1.*

Ébauche de preuve. On doit d'abord, pour le premier critère, argumenter que le protocole est invariant sous la permutation des registres de l'échantillonneur au sens de l'équation (4.5). Remarquons d'abord que le choix de t et c est invariant sous la permutation des positions puisqu'ils sont choisis selon la distribution uniforme. Lorsque Sam envoie t et c à Paul, ce dernier peut calculer la permutation π appliquée à S^N à partir du registre de purification de l'état symétrique $\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}$ et ainsi ajuster son attaque en fonction de π. Il doit ensuite réordonner son résultat de mesure pour qu'il s'aligne correctement avec les systèmes S correspondants du côté de Sam. Cette attaque sur le protocole symétrique est équivalente à l'attaque de Paul sur le protocole régulier, à une permutation près sur les registres de sortie.

Le deuxième critère est un peu plus subtil ; il faut montrer que si l'état conjoint initial est de la forme $|\theta\rangle\langle\theta|_{\mathsf{PS}}^{\otimes N}$, où l'état réduit chez Sam satisfait $F(\theta_{\mathsf{S}}, \frac{1}{2}\mathbb{1}_{\mathsf{S}})^2 < 1 - \epsilon$, alors Paul a probabilité négligeable de passer le test. L'observation cruciale pour la preuve est que le seul état de deux qubits qui est parfaitement

Échantillonnage EPR-OLCC

Paramètres : $N \in \mathbb{N}$ et $\beta \in \mathbb{R}$ tel que $0 < \beta < 1$

1. Paul prépare N paires EPR $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et envoie la moitié de chaque paire à Sam.
2. Sam choisit aléatoirement un échantillon $t \subset_R [N]$ de taille $k = \lceil \beta N \rceil$ et une base $c \in_R \{0,1\}^k$, et il envoie t et c à Paul.
3. À la réception de t et c, Paul mesure chacun de ses qubits appartenant aux positions échantillonnées $i \in t$ dans la base correspondante c_i. Il envoie le résultat de la mesure $\hat{X} \in \{0,1\}^k$ à Sam.
4. Sam mesure chacun de ses qubits échantillonnés dans la base correspondante c_i, soit $X \in \{0,1\}^k$ le résultat de sa mesure. Il rejette si $\hat{X} \neq X$.

FIGURE 4.3 – Le protocole d'échantillonnage avec mesures locales et communication classique pour certifier des demi-paires EPR (état de référence $\varphi = \frac{\mathbb{1}}{2}$).

corrélé à la fois dans la base calculatoire et dans la base diagonale est la paire EPR $|\Phi^+\rangle$. Ainsi, si la fidélité entre l'état conjoint $|\theta\rangle_{\mathsf{PS}}$ et $|\Phi^+\rangle$ est trop basse, alors les résultats de mesure ne peuvent pas être parfaitement corrélés dans les deux bases, sauf avec probabilité négligeable.

Le troisième critère est trivial à montrer puisque ni le protocole réel ni la version symétrique décrite ci-dessus ne touchent les systèmes S non échantillonnés autrement que par une permutation. □

4.4 Analyse des protocoles d'échantillonnage d'états mixtes

Dans cette section, nous analysons les protocoles d'échantillonnage de la forme donnée par la figure 4.2 qui satisfont la définition 4.3.1. Nous montrons que l'état post-échantillonnage de ces protocoles peut s'apparenter à un état idéal par la relation (4.2).

4.4.1 Preuve contre les adversaires symétriques

En considérant les protocoles qui sont invariants sous les permutations au sens de la définition 4.3.1, nous pouvons, comme première étape, utiliser les propriétés des états symétriques pour borner supérieurement la probabilité d'échec de ces protocoles contre les adversaires symétriques, c'est-à-dire contre les

adversaires qui préparent un état initial $|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle$ qui vit dans le sous-espace symétrique $\mathrm{Sym}^N(\mathcal{H}_\mathsf{P}\otimes\mathcal{H}_\mathsf{S})$. Puisque tout adversaire contre un protocole qui satisfait la définition 4.3.1 est équivalent à un adversaire symétrique, à une permutation près sur le registre de sortie de l'échantillonneur, on obtient ainsi un résultat en termes d'état idéal sur l'état post-échantillonnage permuté de Sam contre un adversaire arbitraire.

Le lemme 4.4.1 ci-dessous utilise le fait que les états symétriques sont approximés par une mixture d'états i.i.d. pour montrer que la sortie permutée d'un protocole qui satisfait la définition 4.3.1 est approximée par une mixture d'états qui sont i.i.d. en un état près de l'état de référence φ.

Lemme 4.4.1. *Soit $\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}$ le super-opérateur qui décrit la sortie d'un protocole d'échantillonnage satisfaisant la définition 4.3.1 et soit $\rho_{\mathsf{R}\mathsf{S}^N}\in\mathcal{D}(\mathcal{H}_\mathsf{R}\otimes\mathcal{H}_\mathsf{S}^{\otimes N})$. Pour tout $\epsilon>0$, il existe*

1. *une mesure sous-normalisée $d\theta_\mathsf{S}$ sur l'ensemble des états mixtes $\theta_\mathsf{S}\in\mathcal{D}(\mathcal{H}_\mathsf{S})$ qui satisfont $F(\theta_\mathsf{S},\varphi_\mathsf{S})^2\geq 1-\epsilon$ et*
2. *un opérateur $\tilde{\sigma}_{\mathsf{S}^n}$*

tels que

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n}\pi_{\mathsf{S}^n}\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N})\pi^*_{\mathsf{S}^n}\leq c_{N,d^2}\cdot\int\theta^{\otimes n}_{\mathsf{S}^n}d\theta_\mathsf{S}+\tilde{\sigma}_{\mathsf{S}^n} \tag{4.7}$$

où $\|\tilde{\sigma}_{\mathsf{S}^n}\|_1\leq\mathrm{negl}(N)$ et où c_{N,d^2} est la dimension du sous-espace symétrique $\mathrm{Sym}^N(\mathcal{H}_\mathsf{P}\otimes\mathcal{H}_\mathsf{S})$.

Démonstration. Par la définition 4.3.1, on sait qu'il existe un super-opérateur $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ et un état symétrique $|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle\in\mathrm{Sym}^N(\mathcal{H}_\mathsf{P}\otimes\mathcal{H}_\mathsf{S})$ tels que

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n}|\pi\rangle\langle\pi|_\Pi\otimes\pi_{\mathsf{S}^n}\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N})\pi^*_{\mathsf{S}^n}=\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N})\ . \tag{4.8}$$

Il suffit donc de prouver l'énoncé pour le super-opérateur $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\mathsf{S}^n}$ obtenu en prenant la trace partielle du registre Π de la sortie de $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$.

Puisque $|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle\in\mathrm{Sym}^N(\mathcal{H}_\mathsf{P}\otimes\mathcal{H}_\mathsf{S})$, la proposition 2.8.2 assure que $\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\leq c_{N,d^2}\cdot\int|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N}\,d|\theta\rangle_{\mathsf{P}\mathsf{S}}$ où $d|\theta\rangle_{\mathsf{P}\mathsf{S}}$ est une mesure normalisée sur l'ensemble des états purs sur $\mathcal{H}_\mathsf{P}\otimes\mathcal{H}_\mathsf{S}$. Il en découle que

$$\begin{aligned}
\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\mathsf{S}^n}(\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}) &\leq \bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\mathsf{S}^n}\left(c_{N,d^2}\cdot\int|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N}\,d|\theta\rangle\right)\\
&= c_{N,d^2}\cdot\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\mathsf{S}^n}\Bigg(\int_{\theta_\mathsf{S}\approx^\epsilon\varphi_\mathsf{S}}|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N}\,d|\theta\rangle\\
&\qquad\qquad+\int_{\theta_\mathsf{S}\not\approx^\epsilon\varphi_\mathsf{S}}|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N}\,d|\theta\rangle\Bigg)\\
&\leq c_{N,d^2}\cdot\int_{\theta_\mathsf{S}\approx^\epsilon\varphi_\mathsf{S}}\theta^{\otimes n}_{\mathsf{S}^n}\,d\theta_\mathsf{S}+\tilde{\sigma}_{\mathsf{S}^n}
\end{aligned}$$

où $\theta_{\mathsf{S}} \approx^{\epsilon} \varphi_{\mathsf{S}}$ veut dire que $F(\theta_{\mathsf{S}}, \varphi_{\mathsf{S}})^2 \geq 1-\epsilon$ et où l'opérateur $\tilde{\sigma}_{\mathsf{S}^n} := c_{N,d^2} \cdot \bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N \to \mathsf{S}^n} \left(\int_{\theta \not\approx^{\epsilon} \varphi} |\theta\rangle\langle\theta|^{\otimes N} d|\theta\rangle \right)$ satisfait $\|\tilde{\sigma}_{\mathsf{S}^n}\|_1 \leq \text{negl}(N)$ par le deuxième critère de la définition 4.3.1. La dernière inégalité de l'équation ci-dessus découle du troisième critère de la définition 4.3.1 : puisque le super-opérateur $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N \to \mathsf{S}^n}$ n'agit pas sur les registres non échantillonnés autrement que par une permutation aléatoire, et puisque cette permutation ne change pas l'état $\theta^{\otimes n}$, l'état de S^n *après* l'application de ce super-opérateur est borné supérieurement par l'état de ces mêmes registres *avant* son application.

Pour conclure, remarquons que la mesure $d\theta_{\mathsf{S}}$ est obtenue en prenant la trace partielle du registre P de la mesure $d|\theta\rangle_{\mathsf{PS}}$ sur l'ensemble restreint des états purs $|\theta\rangle_{\mathsf{PS}}$ tels que $F(\theta_{\mathsf{S}}, \varphi_{\mathsf{S}})^2 \geq 1-\epsilon$. Ceci correspond à une mesure sous-normalisée (car prise sur un sous-ensemble des états purs) qui est proportionnelle à la mesure de Hilbert-Schmidt [ZS01, Ren10] sur les opérateurs de densité sur S qui satisfont $F(\theta_{\mathsf{S}}, \varphi_{\mathsf{S}})^2 \geq 1-\epsilon$. □

À partir du lemme ci-dessus, on peut montrer que la sortie permutée du protocole d'échantillonnage est bornée supérieurement par un état presque idéal, dans le même esprit que l'inégalité (4.2). Autrement dit, le corollaire ci-dessous établit qu'un protocole satisfaisant la définition 4.3.1 et sûr si la sortie est permutée aléatoirement.

Corollaire 4.4.1. *Soit $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N \to \mathsf{S}^n}$ le super-opérateur complètement positif qui décrit la sortie d'un protocole d'échantillonnage qui satisfait la définition 4.3.1 et soit $\rho_{\mathsf{RS}^N} \in \mathcal{D}(\mathcal{H}_{\mathsf{R}} \otimes \mathcal{H}_{\mathsf{S}}^{\otimes N})$. Pour tout $\epsilon > 0$, il existe un opérateur sous-normalisé ϵ-idéal $\psi_{\mathsf{S}^n} \in \mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{S}}^{\otimes n})$ et un opérateur σ_{S^n} tels que*

$$\frac{1}{n!} \sum_{\pi \in \mathcal{S}_n} \pi_{\mathsf{S}^n} \mathcal{E}^{\text{acc}}_{\mathsf{RS}^N \to \mathsf{S}^n}(\rho_{\mathsf{RS}^N}) \pi^*_{\mathsf{S}^n} \leq c_{N,d^2} \cdot \psi_{\mathsf{S}^n} + \sigma_{\mathsf{S}^n} \tag{4.9}$$

où $\|\sigma_{\mathsf{S}^n}\|_1 \leq \text{negl}(N)$.

La preuve du corollaire se base essentiellement sur le lemme suivant qui énonce qu'un état composé de n copies i.i.d. d'un état près de $|\nu\rangle$ est presque entièrement contenu dans la sphère de Hamming quantique autour de $|\nu\rangle^{\otimes n}$.

Lemme 4.4.2. *Soient $\epsilon > 0$ et $|\nu\rangle, |\theta\rangle \in \mathcal{H}$ tels que $|\langle\theta|\nu\rangle|^2 \geq 1-\epsilon$. Alors pour tout $n \in \mathbb{N}$, $\alpha > 0$ et pour $r = (\epsilon + \alpha)n$,*

$$\text{tr}\left(\mathbb{P}^{r,|\nu\rangle} \cdot |\theta\rangle\langle\theta|^{\otimes n} \right) \geq 1 - \exp(-2\alpha^2 n)$$

où $\mathbb{P}^{r,|\nu\rangle}$ est le projecteur sur $\Delta_r(|\nu\rangle^{\otimes n})$.

Démonstration. Observons d'abord que

$$\text{tr}\left(\mathbb{P}^{r,|\nu\rangle} |\theta\rangle\langle\theta|^{\otimes n} \right) = \Pr[wt(X_\theta) \leq r] = \Pr[wt(X_\theta) - \epsilon n \leq \alpha n] \tag{4.10}$$

où X_θ est la variable aléatoire résultant de la mesure des n copies de $|\theta\rangle$ avec les opérateurs de mesure $M_0 = |\nu\rangle\langle\nu|$ et $M_1 = \mathbb{1} - |\nu\rangle\langle\nu|$. Autrement dit, X_θ est composée de n variables Bernoulli de paramètre $\mathrm{tr}((\mathbb{1} - |\nu\rangle\langle\nu|) \cdot |\theta\rangle\langle\theta|) = 1 - |\langle\theta|\nu\rangle|^2 \leq \epsilon$. L'inégalité d'Hoeffding (théorème 2.2.1) nous permet donc de borner inférieurement la quantité (4.10) par $1 - \exp(-2\alpha^2 n)$. □

Preuve du corollaire 4.4.1. Posons $\gamma = \epsilon/2$ et soient $d\theta_{\mathsf{S}}$ et $\tilde{\sigma}_{\mathsf{S}^n}$ tels que définis dans l'énoncé du lemme 4.4.1 avec paramètre γ, c'est-à-dire tels que

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{\mathsf{S}^n}\mathcal{E}^{\mathrm{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N})\pi^*_{\mathsf{S}^n} \leq c_{N,d^2}\cdot\int \theta^{\otimes n}_{\mathsf{S}^n} d\theta_{\mathsf{S}} + \tilde{\sigma}_{\mathsf{S}^n} \tag{4.11}$$

où $d\theta_{\mathsf{S}}$ est une mesure sous-normalisée sur l'ensemble des états mixtes sur S qui satisfont $F(\theta_{\mathsf{S}}, \varphi_{\mathsf{S}})^2 \geq 1-\gamma$ et où $\tilde{\sigma}_{\mathsf{S}^n}$ a une norme de trace négligeable.

Soit $\tau_{\mathsf{P}^n\mathsf{S}^n} := \int |\theta\rangle\langle\theta|^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n} d\theta_{\mathsf{S}}$ une extension de $\int \theta^{\otimes n}_{\mathsf{S}^n} d\theta_{\mathsf{S}}$ où chaque $|\theta\rangle_{\mathsf{PS}}$ est tel que $|\langle\theta_{\mathsf{PS}}|\varphi_{\mathsf{PS}}\rangle|^2 = F(\theta_{\mathsf{S}}, \varphi_{\mathsf{S}})^2 \geq 1-\gamma$ et soit $\tilde{\sigma}_{\mathsf{P}^n\mathsf{S}^n}$ une extension de $\tilde{\sigma}_{\mathsf{S}^n}$. Alors, le lemme 4.4.2 nous dit que

$$\mathrm{tr}\left((\mathbb{1} - \mathbb{P}^{2\gamma n,|\varphi\rangle}_{\mathsf{P}^n\mathsf{S}^n})\,(\tau_{\mathsf{P}^n\mathsf{S}^n})\right) \leq \exp(-2\gamma^2 n)\ . \tag{4.12}$$

Choisissons maintenant $\psi_{\mathsf{S}^n} = \mathrm{tr}_{\mathsf{P}^n}(\mathbb{P}^{2\gamma n,|\varphi\rangle}_{\mathsf{P}^n\mathsf{S}^n}\tau_{\mathsf{P}^n\mathsf{S}^n}\mathbb{P}^{2\gamma n,|\varphi\rangle}_{\mathsf{P}^n\mathsf{S}^n})$. Alors en utilisant (4.11), nous avons que

$$\begin{aligned}\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{\mathsf{S}^n}\mathcal{E}^{\mathrm{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{R\mathsf{S}^N})\pi^*_{\mathsf{S}^n} &\leq c_{N,d^2}\cdot\int \theta^{\otimes n}_{\mathsf{S}^n} d\theta_{\mathsf{S}} + \tilde{\sigma}_{\mathsf{S}^n}\\ &= \mathrm{tr}_{\mathsf{P}^n}\left(c_{N,d^2}\cdot\tau_{\mathsf{P}^n\mathsf{S}^n} + \tilde{\sigma}_{\mathsf{P}^n\mathsf{S}^n}\right) = c_{N,d^2}\cdot\psi_{\mathsf{S}^n} + \sigma_{\mathsf{S}^n}\end{aligned}$$

où la norme de trace de $\sigma_{\mathsf{S}^n} := \mathrm{tr}_{\mathsf{P}^n}(c_{N,d^2}(\tau_{\mathsf{P}^n\mathsf{S}^n} - \mathbb{P}^{2\gamma n,|\varphi\rangle}_{\mathsf{P}^n\mathsf{S}^n}\tau_{\mathsf{P}^n\mathsf{S}^n}\mathbb{P}^{2\gamma n,|\varphi\rangle}) + \tilde{\sigma}_{\mathsf{P}^n\mathsf{S}^n})$ peut être bornée supérieurement par

$$\|\sigma_{\mathsf{P}^n\mathsf{S}^n}\|_1 \leq c_{N,d^2}\|\tau_{\mathsf{P}^n\mathsf{S}^n} - \mathbb{P}^{2\gamma n,|\varphi\rangle}_{\mathsf{P}^n\mathsf{S}^n}\ \tau_{\mathsf{P}^n\mathsf{S}^n}\ \mathbb{P}^{2\gamma n,|\varphi\rangle}_{\mathsf{P}^n\mathsf{S}^n}\|_1 + \|\tilde{\sigma}_{\mathsf{P}^n\mathsf{S}^n}\|_1 \leq \mathrm{negl}(N)$$

en appliquant d'abord l'inégalité du triangle et ensuite le *Gentle Measurement Lemma* (le lemme 2.3.2) avec la borne de (4.12). □

Une conséquence de la définition de l'opérateur σ_{S^n} dans la preuve du corollaire ci-dessus est que ce n'est pas un opérateur positif semi-défini en général. Mais puisque sa norme de trace est négligeable, ce fait ne devrait pas importer pour la plupart des applications, car le côté droit de l'inégalité (4.9) se comporte de manière indistinguable de $c_{N,d^2}\cdot\psi_{\mathsf{S}^n}$.

4.4.2 Preuve contre les adversaires arbitraires : dépermuter la sortie

Afin de conclure que les protocoles d'échantillonnage qui satisfont la définition 4.3.1 fonctionnent comme voulu, il faut montrer qu'une relation de la forme de (4.9) tient, même lorsqu'on retire la permuta-

tion aléatoire de la sortie de $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N \to \mathsf{S}^n}$. Il se trouve que l'énoncé assez intuitif « si l'état de sortie permuté est approximé par un état idéal, alors l'état de sortie non permuté l'est aussi » est assez délicat à démontrer. Nous insistons sur le fait que cette étape est nécessaire si nous voulons un protocole d'échantillonnage naturel qui ne requiert pas de physiquement permuter les registres et qui reste sûr dans les applications où une telle permutation n'est pas permise.

Le lemme 4.4.3 ci-dessous est la première étape de cette preuve. Ce lemme montre que la propriété d'être idéal, c'est-à-dire d'admettre une purification dans un sous-espace à peu d'erreurs, est une propriété invariante sous la permutation, ou plutôt sous la « dépermutation », des registres.

Lemme 4.4.3. *Soit $\epsilon > 0$ et soit $\sigma_{\mathsf{S}^n} \in \mathcal{D}(\mathcal{H}_{\mathsf{S}}^{\otimes n})$ tels que $\frac{1}{n!}\sum_{\pi \in \mathcal{S}_n} \pi_{\mathsf{S}^n} \sigma_{\mathsf{S}^n} \pi^*_{\mathsf{S}^n}$ est ϵ-idéal, alors σ_{S^n} est aussi ϵ-idéal.*

Démonstration. Soit $r = \epsilon n$. On doit montrer que si $\bar{\sigma}_{\mathsf{S}^n} := \frac{1}{n!}\sum_{\pi \in \mathcal{S}_n} \pi_{\mathsf{S}^n} \sigma_{\mathsf{S}^n} \pi^*_{\mathsf{S}^n}$ a une purification dans $\mathcal{H}_{\mathsf{R}} \otimes \Delta_r(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$ pour un certain registre R, alors σ_{S^n} a aussi une telle purification dans $\mathcal{H}_{\mathsf{R}} \otimes \Delta_r(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$. Soit $|\bar{\sigma}_{\mathsf{RP}^n\mathsf{S}^n}\rangle \in \mathcal{H}_{\mathsf{R}} \otimes \Delta_r(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$ la purification de $\bar{\sigma}_{\mathsf{S}^n}$ qui existe par supposition et soit $\sum_i p_i |i_{\mathsf{S}^n}\rangle\langle i_{\mathsf{S}^n}|$ la décomposition spectrale de σ_{S^n}. Définissons l'état pur

$$|\bar{\sigma}_{\Pi\mathsf{P}^n\mathsf{S}^n}\rangle = \sqrt{\frac{1}{n!}} \sum_{\pi \in \mathcal{S}_n} |\pi\rangle_{\Pi} \otimes \left(\sum_i \sqrt{p_i} |i_{\mathsf{P}^n}\rangle \otimes \pi_{\mathsf{S}^n} |i_{\mathsf{S}^n}\rangle \right)$$

où $\{|i_{\mathsf{P}^n}\rangle\}_i$ est une base de $\mathcal{H}_{\mathsf{P}^n}$. Remarquons que cet état est une purification de $\bar{\sigma}_{\mathsf{S}^n}$, donc il existe une isométrie $V_{\Pi\mathsf{P}^n \to \mathsf{RP}^n}$ telle que $V_{\Pi\mathsf{P}^n \to \mathsf{RP}^n} |\bar{\sigma}_{\Pi\mathsf{P}^n\mathsf{S}^n}\rangle = |\bar{\sigma}_{\mathsf{RP}^n\mathsf{S}^n}\rangle \in \mathcal{H}_{\mathsf{R}} \otimes \Delta_r(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$. On peut exprimer $|\bar{\sigma}_{\mathsf{RP}^n\mathsf{S}^n}\rangle$ comme :

$$\begin{aligned} |\bar{\sigma}_{\mathsf{RP}^n\mathsf{S}^n}\rangle &= (V_{\Pi\mathsf{P}^n \to \mathsf{RP}^n} \otimes \mathbb{1}_{\mathsf{S}^n}) |\sigma_{\Pi\mathsf{P}^n\mathsf{S}^n}\rangle \\ &= \sum_{\pi,i} \sqrt{\frac{p_i}{n!}} V_{\Pi\mathsf{P}^n \to \mathsf{RP}^n} |\pi\rangle_{\Pi} |i_{\mathsf{P}^n}\rangle \otimes \pi_{\mathsf{S}^n} |i_{\mathsf{S}^n}\rangle = \sum_{\pi,i} \sqrt{\frac{p_i}{n!}} |\xi_{\pi,i}\rangle_{\mathsf{RP}^n} \otimes \pi_{\mathsf{S}^n} |i_{\mathsf{S}^n}\rangle \end{aligned}$$

où les vecteurs $|\xi_{\pi,i}\rangle_{\mathsf{RP}^n} := V_{\Pi\mathsf{P}^n \to \mathsf{RP}^n} |\pi\rangle_{\Pi} |i_{\mathsf{P}^n}\rangle$ sont orthogonaux deux à deux. En extrayant la permutation π des registres RP^n et en défaisant cette permutation sur les registres P^n et S^n, on obtient l'état

$$\sum_{\pi,i} \sqrt{\frac{p_i}{n!}} (\mathbb{1}_{\mathsf{R}} \otimes \pi^{-1}_{\mathsf{P}^n}) |\xi_{\pi,i}\rangle_{\mathsf{RP}^n} \otimes |i_{\mathsf{S}^n}\rangle \tag{4.13}$$

Notons que l'action sur $\mathsf{RP}^n\mathsf{S}^n$ décrite plus haut est isométrique et que, avant et après l'application de cette isométrie, l'état des registres P^n et S^n a support dans le sous-espace $\Delta_r(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$ puisque ce celui-ci est invariant sous la permutation des registres PS. La preuve est complétée puisque l'état (4.13) est une purification de σ_{S^n} qui appartient au sous-espace $\mathcal{H}_{\mathsf{R}} \otimes \Delta_r(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$. □

Nous avons maintenant tous les outils nécessaires pour prouver notre résultat principal, le théorème 4.4.1 ci-dessous. Sa preuve combine le corollaire 4.4.1 et le lemme 4.4.3 pour montrer que la sortie du

protocole d'échantillonnage est arbitrairement près d'un état post-sélectionné sur le registre de purification d'un état idéal.

Théorème 4.4.1. *Soit $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$ la sortie d'un protocole d'échantillonnage qui satisfait la définition 4.3.1 et soit $\rho_{\mathsf{RS}^N} \in \mathcal{D}(\mathcal{H}_{\mathsf{R}} \otimes \mathcal{H}_{\mathsf{S}}^{\otimes N})$. Pour tout $\epsilon > 0$, il existe un vecteur sous-normalisé*

$$\left|\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\right\rangle \in \mathcal{H}_{\mathsf{R}'} \otimes \Delta_{\epsilon n}(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$$

et un CPTN $\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n\to\mathbb{C}}$ tels que

$$\left\|\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N}) - c_{N,d^2}(\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n} \otimes \mathrm{id}_{\mathsf{S}^n})(\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n})\right\|_1 \leq \mathrm{negl}(N)$$

Démonstration. Soient ψ_{S^n} et σ_{S^n} tels que définis dans l'énoncé du corollaire 4.4.1, c'est-à-dire tels que

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \pi_{\mathsf{S}^n}\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N})\pi^*_{\mathsf{S}^n} \leq c_{N,d^2}\cdot\psi_{\mathsf{S}^n} + \sigma_{\mathsf{S}^n} \tag{4.14}$$

et où $\|\sigma_{\mathsf{S}^n}\|_1 \leq \mathrm{negl}(N)$. Définissons l'opérateur $\tau_{\mathsf{S}^n} := \psi_{\mathsf{S}^n} + c^{-1}_{N,d^2}\cdot\sigma_{\mathsf{S}^n}$ qui correspond à la partie droite de (4.14) multipliée par le facteur c^{-1}_{N,d^2}. Puisque ψ_{S^n} est ϵ-idéal, il existe une purification de ψ_{S^n} qui vit dans le sous-espace à peu d'erreurs $\mathcal{H}_{\mathsf{R}'} \otimes \Delta_{\epsilon n}(|\varphi\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$, soit $|\psi_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\rangle$ cette purification. Par la proposition 2.3.2, il existe une purification $|\tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\rangle$ de τ_{S^n} telle que $\|\psi_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n} - \tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\|_1 \leq \mathrm{negl}(N)$. À partir de (4.14) et de la proposition 2.9.1 on peut montrer qu'il existe un super-opérateur complètement positif $\mathcal{K}_{\mathsf{R}'\mathsf{P}^n\to\Pi}$ qui produit un registre classique Π à partir des registres de purification $\mathsf{R}'\mathsf{P}^n$ avec la propriété que

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} |\pi\rangle\langle\pi|_\Pi \otimes \pi_{\mathsf{S}^n}\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N})\pi^*_{\mathsf{S}^n} = c_{N,d^2}(\mathcal{K}_{\mathsf{R}'\mathsf{P}^n\to\Pi} \otimes \mathrm{id}_{\mathsf{S}^n})(\tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}) \ . \tag{4.15}$$

Supposons maintenant qu'on soumette les deux côtés de l'égalité ci-dessus à l'opération quantique suivante : mesurer le registre Π et défaire la permutation ainsi observée sur le registre S^n. Le côté gauche de (4.15) deviendrait $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N})$, tandis que le côté droit deviendrait

$$c_{N,d^2}\cdot\sum_{\pi\in\mathcal{S}_n}(\langle\pi|_\Pi \otimes \pi^{-1}_{\mathsf{S}^n})(\mathcal{K}_{\mathsf{R}'\mathsf{P}^n\to\Pi} \otimes \mathrm{id}_{\mathsf{S}^n})(\tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n})(|\pi\rangle_\Pi \otimes (\pi^{-1}_{\mathsf{S}^n})^*) \ .$$

Nous montrons maintenant comment représenter cet opérateur d'une manière qui correspond à l'énoncé que nous souhaitons prouver, c'est-à-dire comme un opérateur post-sélectionné sur le registre de purification d'un état presque idéal. Dans ce but, définissons [3] une isométrie $U_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}\Pi}$ qui purifie l'action de

3. Il est toujours possible de définir une isométrie et un projecteur de ce type pour n'importe quel super-opérateur complètement positif $\mathcal{E}_{\mathsf{A}\to\mathsf{B}}$. En effet, soit $\mathcal{E}(\sigma_\mathsf{A}) = \sum_k E_k\sigma_\mathsf{A}E_k^*$ où $E_k \in L(\mathcal{H}_\mathsf{A}, \mathcal{H}_\mathsf{B})$ sont les opérateurs de Kraus de $\mathcal{E}$ et définissons l'isométrie $U_{\mathsf{A}\to\mathsf{BZ}}$ qui transforme un état pur arbitraire $|\psi\rangle_\mathsf{A}$ en $\sum_k E_k|\psi\rangle_\mathsf{A}|k\rangle_\mathsf{Z} + \sqrt{\mathbb{1} - \sum_k E_k^*E_k}|\psi\rangle_\mathsf{A}|\perp\rangle_\mathsf{Z}$ où $|\perp\rangle_\mathsf{Z}$ est choisi comme étant orthogonal à $|k\rangle_\mathsf{Z}$ pour tout k. Alors $\mathbb{P}_\mathsf{Z} = \sum_k |k\rangle\langle k|_\mathsf{Z}$ est le projecteur qui complète cette représentation de $\mathcal{E}$ car $\mathrm{tr}_\mathsf{Z}((\mathbb{1}_\mathsf{B} \otimes \mathbb{P}_\mathsf{Z})U_{\mathsf{A}\to\mathsf{BZ}}\sigma_\mathsf{A}U^*_{\mathsf{A}\to\mathsf{BZ}}) = \sum_k E_k\sigma_\mathsf{A}E_k^* = \mathcal{E}_{\mathsf{A}\to\mathsf{B}}(\sigma_\mathsf{A})$.

$\mathcal{K}_{\mathsf{R}'\mathsf{P}^n\to\Pi}$, c'est-à-dire telle que pour n'importe quel état $\nu_{\mathsf{R}'\mathsf{P}^n}$,

$$\mathcal{K}_{\mathsf{R}'\mathsf{P}^n\to\Pi}(\nu_{\mathsf{R}'\mathsf{P}^n}) := \mathrm{tr}_{\mathsf{Z}}\left((\mathbb{P}_{\mathsf{Z}}\otimes\mathbb{1}_{\Pi})\cdot U_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}\Pi}\cdot\nu_{\mathsf{R}'\mathsf{P}^n}\cdot(U_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}\Pi})^*\right)$$

pour un certain projecteur $\mathbb{P}_{\mathsf{Z}}$. En utilisant cette représentation, l'opérateur post-échantillonnage peut être exprimé comme

$$\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N}) = c_{N,d^2}\cdot\mathrm{tr}_{\mathsf{Z}}\left((\mathbb{P}_{\mathsf{Z}}\otimes\mathbb{1}_{\mathsf{S}^n})\cdot\sum_{\pi\in\mathcal{S}_n}[U^{\pi}_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}}\otimes\pi^{-1}_{\mathsf{S}^n}](\tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n})\right) \tag{4.16}$$

où $U^{\pi}_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}} := (\mathbb{1}_{\mathsf{Z}}\otimes\langle\pi|_{\Pi})\cdot U_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}\Pi}$ et où $[U](\rho)$ est une notation concise pour $U\rho U^*$.

Définissons l'opérateur

$$\tilde{\psi}_{\mathsf{Z}\mathsf{S}^n} := \sum_{\pi\in\mathcal{S}_n}(U^{\pi}_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}}\otimes\pi^{-1}_{\mathsf{S}^n})\psi_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}(U^{\pi}_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}}\otimes\pi^{-1}_{\mathsf{S}^n})^* \ .$$

où $\psi_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}$ est la purification de ψ_{S^n} définie plus haut. En utilisant le fait que ψ_{S^n} est invariant sous les permutations, on remarque que $\tilde{\psi}_{\mathsf{S}^n}$ est tel que $\psi_{\mathsf{S}^n} = \frac{1}{n!}\sum_{\pi\in\mathcal{S}_n}\pi_{\mathsf{S}^n}\tilde{\psi}_{\mathsf{S}^n}\pi^*_{\mathsf{S}^n}$. Puisque ψ_{S^n} a une purification dans le sous-espace à peu d'erreurs, le lemme 4.4.3 implique que $\tilde{\psi}_{\mathsf{S}^n}$ admet aussi une purification dans ce sous-espace. Soit $|\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\rangle$ cette purification et soit $\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n\to\mathbb{C}}$ le super-opérateur qui envoie d'abord $|\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\rangle$ vers $\tilde{\psi}_{\mathsf{Z}\mathsf{S}^n}$ et qui applique ensuite l'opération $\sigma_{\mathsf{Z}}\mapsto\mathrm{tr}_{\mathsf{Z}}(\mathbb{P}_{\mathsf{Z}}\sigma_{\mathsf{Z}})$ au registre Z. Alors, en utilisant la définition de $\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}$ et de $\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n}$, et puisque les opérations quantiques n'augmentent pas la norme de trace, nous avons que

$$\begin{aligned}
&\left\|\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N}) - c_{N,d^2}(\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n}\otimes\mathrm{id}_{\mathsf{S}^n})(\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n})\right\|_1\\
=&\left\|c_{N,d^2}\cdot\mathrm{tr}_{\mathsf{Z}}\left((\mathbb{P}_{\mathsf{Z}}\otimes\mathbb{1}_{\mathsf{S}^n})\cdot\sum_{\pi\in\mathcal{S}_n}[U^{\pi}_{\mathsf{R}'\mathsf{P}^n\to\mathsf{Z}}\otimes\pi^{-1}_{\mathsf{S}^n}]\Big(\tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}-\psi_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\Big)\right)\right\|_1\\
\leq& c_{N,d^2}\cdot\|\tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}-\psi_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\|_1\\
\leq&\,\mathrm{negl}(N)
\end{aligned}$$

où dans première inégalité, $\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N})$ est remplacé par (4.16) et la dernière inégalité découle de notre choix de $|\tau_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\rangle$. □

À l'aide de la remarque 2.9.1, on peut exprimer le résultat du théorème 4.4.1 en une inégalité d'opérateurs, tel que suggéré par l'équation (4.2) de la section 4.2, plutôt que par post-sélection. En fait, la proposition 2.9.1 montre que ces deux points de vue sont équivalents.

Corollaire 4.4.2. *Soit $\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}$ la sortie d'un protocole d'échantillonnage qui satisfait la définition 4.3.1 et soit $\rho_{\mathsf{R}\mathsf{S}^N}\in\mathcal{D}(\mathcal{H}_{\mathsf{R}}\otimes\mathcal{H}_{\mathsf{S}}^{\otimes N})$. Pour tout $\epsilon>0$, il existe un opérateur sous-normalisé ϵ-idéal $\psi_{\mathsf{S}^n}\in\mathcal{D}_{\leq}(\mathcal{H}_{\mathsf{S}}^{\otimes n})$ et un opérateur σ_{S^n} tels que*

$$\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N})\leq c_{N,d^2}\cdot\psi_{\mathsf{S}^n}+\sigma_{\mathsf{S}^n}$$

où $\|\sigma_{\mathsf{S}^n}\|_1 \leq \mathrm{negl}(N)$.

Démonstration. Soient $|\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}\rangle$ et $\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n\to\mathbb{C}}$ comme dans l'énoncé du théorème 4.4.1. Alors

$$\begin{aligned}\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N}) &= c_{N,d^2}(\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n})(\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n}) + \sigma_{\mathsf{S}^n}\\ &\leq c_{N,d^2}\cdot\psi_{\mathsf{S}^n} + \sigma_{\mathsf{S}^n}\end{aligned}$$

où $\sigma_{\mathsf{S}^n} := \mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N}) - c_{N,d^2}\tilde{\mathcal{K}}_{\mathsf{R}'\mathsf{P}^n}(\tilde{\psi}_{\mathsf{R}'\mathsf{P}^n\mathsf{S}^n})$ a norme négligeable en N par le théorème 4.4.1 et où l'inégalité ci-dessus découle de la remarque 2.9.1. □

4.5 Génération sûre d'aléa partagé

Dans cette section, nous appliquons les résultats que nous avons vus jusqu'ici dans ce chapitre au problème de *génération d'aléa partagé*. Ce problème peut être vu comme une généralisation du problème de tirage d'une pièce où, au lieu de vouloir générer un seul bit commun avec le plus petit biais possible, les deux participants Alice et Bob veulent plutôt générer une chaine de bits commune de taille n qui est le plus près possible d'uniformément distribuée. Plus formellement, nous investiguons quelle est la plus grande quantité d'incertitude, mesurée par la min-entropie, qu'Alice et Bob peuvent générer par un protocole quantique sans hypothèse. Nous montrons qu'il est possible de générer une chaine pour laquelle la min-entropie est presque maximale avec probabilité $1 - \mathrm{negl}(N)$, à l'aide d'un protocole qui se sert de notre résultat d'échantillonnage pour certifier des demi-paires EPR et utilise ces paires pour générer l'aléa. Plus précisément, nous montrons le théorème suivant.

Théorème 4.5.1. *Il existe un protocole quantique entre Alice et Bob tel que pour tout* $\gamma > 0$*,*

- *si Alice et Bob sont honnêtes, leurs sorties respectives* $X_A \in \{0,1\}^n$ *et* $X_B \in \{0,1\}^n$ *satisfont* $X_A = X_B$*,*
- *si Alice est honnête, alors* $\mathrm{H}_\infty(X_A) \geq (1-\gamma)n$*, sauf avec probabilité négligeable en* n*, et*
- *si Bob est honnête, alors* $\mathrm{H}_\infty(X_B) \geq (1-\gamma)n$*, sauf avec probabilité négligeable en* n*.*

4.5.1 Le protocole

Le protocole de génération d'aléa partagé est décrit dans la figure 4.4. Le protocole demande à Alice de préparer N paires EPR et d'envoyer la moitié de chacune à Bob. Bob utilise ensuite un protocole d'échantillonnage d'état mixte (par exemple, celui de la figure 4.1 ou encore de la figure 4.3) pour certifier qu'Alice lui a bien envoyé l'état $\varphi = \frac{\mathbb{1}}{2}$ pour la plupart des positions. Si Bob accepte le résultat de

l'échantillonnage, alors il sait qu'il partage un état qui n'est pas trop loin de celui qu'Alice devait préparer. Le résultat de sa mesure aura alors une très haute min-entropie.

Paramètres : $N \in \mathbb{N}$ et $\beta \in \mathbb{R}$ tel que $0 < \beta < 1$ et tel que $\beta N \in \mathbb{N}$

1. Alice prépare l'état $|\Phi^+\rangle_{\mathsf{A}^N\mathsf{B}^N}^{\otimes N}$ pour $|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et envoie le système B^N à Bob.
2. Alice et Bob exécutent un protocole d'échantillonnage d'états mixtes qui satisfait la définition 4.3.1 avec Alice comme prouveuse et Bob comme échantillonneur et avec les paramètres N et β pour l'état de référence $\varphi = \frac{\mathbb{1}}{2}$. Soit $\rho_{\mathsf{A}^n\mathsf{B}^n} \in \mathcal{D}((\mathcal{H}_2 \otimes \mathcal{H}_2)^{\otimes n})$ l'état de $n = N - \beta N$ paires de qubits conditionné sur le fait que Bob accepte l'échantillonnage.
3. Alice et Bob mesurent leurs n qubits respectifs dans la base calculatoire et produisent respectivement les sorties X_A et X_B.

FIGURE 4.4 – Le protocole de génération sûre d'aléa partagé. N est le paramètre de sécurité, β détermine la taille de l'échantillon et $n = N - \beta N$ est la taille de la sortie.

4.5.2 Preuve du théorème 4.5.1

Il est clair que le premier point du théorème 4.5.1 est satisfait si les deux participants sont honnêtes. Dans cette section, nous allons montrer que la min-entropie du résultat de mesure de chacun des participants est arbitrairement près de maximale, sauf avec probabilité négligeable, même si l'autre participant est malhonnête (lemmes 4.5.1 et 4.5.3).

Puisqu'Alice est celle qui prépare les N paires EPR, il n'est pas trop dur de montrer que sa sortie aura une très grande min-entropie. La partie délicate de la preuve est de montrer que les interactions que Bob peut utiliser pour biaiser la sortie d'Alice — le choix de t et d'accepter ou de refuser le résultat de l'échantillonnage — ne peuvent pas trop influencer la distribution de X_A.

Lemme 4.5.1 (Min-entropie de la sortie d'Alice)**.** *Si Alice est honnête, alors pour tout $\gamma > 0$, sa sortie $X_A \in \{0,1\}^n$ satisfait*

$$\mathrm{H}_\infty(X_A) \geq (1-\gamma)n \ ,$$

sauf avec probabilité négligeable en n.

Démonstration. Soit $\rho_{\mathsf{A}^N\mathsf{B}^N}$ l'état conjoint d'Alice et de Bob avant la phase d'échantillonnage. Puisqu'Alice prépare l'état et qu'elle est honnête, elle prépare N paires EPR parfaites (c'est-à-dire $\rho_{\mathsf{A}^N\mathsf{B}^N} = |\Phi^+\rangle\langle\Phi^+|^{\otimes N}$). Donc son résultat de mesure à la fin du protocole aurait min-entropie maximale si on

ignorait les actions de Bob. Bob peut biaiser la sortie d'Alice de deux façons : (1) il peut mesurer son registre B^N *avant* de choisir t et faire dépendre t du résultat de cette mesure, et (2) il peut faire avorter le protocole en rejetant l'échantillonnage, même si Alice prépare le bon état. Nous analysons les deux cas séparément, et montrons que pour chacun, les actions de Bob ne peuvent faire diminuer la min-entropie de X_A par plus qu'une petite quantité, sauf avec probabilité négligeable.

Pour le cas (1), supposons que Bob effectue une mesure sur son registre B^N qui mène à un choix d'échantillon $t \subset [N]$ avec probabilité p_t et qui donne l'état réduit conditionné $\rho^t_{\mathsf{A}^N}$ sur le registre d'Alice. Supposons aussi qu'Alice mesure l'ensemble de ses qubits à cette étape du protocole, donnant lieu au résultat $X_A \in \{0,1\}^N$. Observons que, par la loi des probabilités totales,

$$2^{-N} = 2^{-\mathrm{H}_\infty(X_A)_\rho} = \sum_t p_t \cdot 2^{-\mathrm{H}_\infty(X_A|T=t)_{\rho^t}} \quad ,$$

puisque $2^{-\mathrm{H}_\infty(X_A|T=t)_{\rho^t}}$ correspond à la probabilité maximale de deviner la valeur que prend X_A conditionné sur l'évènement $T = t$, autrement dit lorsque X_A est obtenu en mesurant $\rho^t_{\mathsf{A}^N}$. Par l'inégalité de Markov, on a que

$$\sum_t p_t \cdot [\mathrm{H}_\infty(X_A|T=t)_{\rho^t} \leq N - (\alpha N)] \leq 2^{-\alpha N}$$

où la notation « $[\cdot]$ » dans l'équation ci-dessus représente le crochet d'Iverson (qui prend la valeur 1 si le contenu est vrai et 0 sinon). Autrement dit, les valeurs de t pour lesquelles $\mathrm{H}_\infty(X_A|T=t)_{\rho^t}$ est plus petit que $(1-\alpha)N$ ont probabilité totale plus petite que $2^{-\alpha N}$.

Souvenons-nous que dans le protocole, Alice ne mesure pas l'ensemble de ses qubits, mais seulement les positions qui n'appartiennent pas à l'échantillon t. Alors soit $X^{\bar{t}}_A$ le résultat de mesure de ces qubits et soit X^t_A le résultat de mesure pour les positions qui appartiennent à t (de telle manière que X_A est composé de $X^{\bar{t}}_A$ et de X^t_A). L'énoncé suivant est vrai, sauf avec probabilité négligeable sur le choix de t :

$$\mathrm{H}_\infty(X^{\bar{t}}_A|T=t) \geq \mathrm{H}_\infty(X_A|T=t, X^t_A) \geq (1-\alpha-\beta)N \tag{4.17}$$

où la dernière inégalité découle de la règle de chaine pour la min-entropie avec $\mathrm{H}_0(X^t_A) = \beta N$.

Pour analyser le deuxième cas (2), observons simplement que

$$2^{-\mathrm{H}_\infty(X^{\bar{t}}_A|T=t,\mathrm{acc})} \leq 2^{-\mathrm{H}_\infty(X^{\bar{t}}_A|T=t)} / \Pr[\mathrm{acc}] \leq 2^{-\mathrm{H}_\infty(X^{\bar{t}}_A|T=t)+\alpha N} \tag{4.18}$$

dès que $\Pr[\mathrm{acc}] \geq 2^{-\alpha N}$ où acc est l'évènement où Bob accepte l'échantillonnage. Donc Bob ne peut réduire la min-entropie de la sortie d'Alice par une quantité linéaire en N en faisant avorter le protocole que si sa probabilité d'accepter est négligeable.

On peut conclure que, sauf avec probabilité négligeable bornée supérieurement par $2 \cdot 2^{-\alpha N}$, la min-entropie du résultat de mesure d'Alice sera au moins

$$\mathrm{H}_\infty(X^{\bar{t}}_A|T=t,\mathrm{acc}) \geq (1-2\alpha-\beta)N \leq (1-2\alpha)(1-\beta)N = (1-2\alpha)n$$

en combinant les bornes de (4.17) et de (4.18) et les probabilités respectives que ces bornes soient vraies. L'énoncé du lemme est obtenu en posant $\alpha = \gamma/2$. □

Le lemme suivant servira à borner inférieurement la min-entropie de la sortie de Bob. Il dit que si l'état conjoint d'Alice et de Bob vit dans le sous-espace à peu d'erreurs définit par la sphère de hamming quantique autour de n paires EPR, alors l'état réduit de Bob a une min-entropie presque maximale.

Lemme 4.5.2. *Soit $\epsilon > 0$ et $|\sigma\rangle_{\mathsf{RP}^n\mathsf{S}^n} \in \mathcal{H}_{\mathsf{R}} \otimes \Delta_{\epsilon n}(|\Phi^+\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$. Alors la min-entropie de l'état réduit σ_{S^n} satisfait*

$$\mathrm{H}_\infty(\mathsf{S}^n)_\sigma \geq (1 - \epsilon - h(\epsilon))n \ .$$

Démonstration. Soit $\Pi_\epsilon = \{E \subseteq [n] : |E| \leq \epsilon n\}$ et soit $\mathbb{P}^{\epsilon n, |\Phi^+\rangle}_{\mathsf{P}^n\mathsf{S}^n} = \sum_{E\in\Pi_\epsilon} \mathbb{P}^E_{\mathsf{P}^n\mathsf{S}^n}$ le projecteur sur le sous-espace $\Delta_{\epsilon n}(|\Phi^+\rangle^{\otimes n}_{\mathsf{P}^n\mathsf{S}^n})$ où

$$\mathbb{P}^E_{\mathsf{P}^n\mathsf{S}^n} = \bigotimes_{i\in E}(\mathbb{1} - \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|)_{\mathsf{P}_i\mathsf{S}_i} \bigotimes_{i\notin E} \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|_{\mathsf{P}_i\mathsf{S}_i} \ .$$

Définissons $|\tilde{\sigma}^E\rangle_{\mathsf{RP}^n\mathsf{S}^n} = (\mathbb{1}_{\mathsf{R}} \otimes \mathbb{P}^E_{\mathsf{P}^n\mathsf{S}^n})|\sigma\rangle_{\mathsf{RP}^n\mathsf{S}^n}$ pour chaque $E \in \Pi_\epsilon$. Par la proposition 2.9.2, on a que

$$|\sigma\rangle\!\langle\sigma|_{\mathsf{RP}^n\mathsf{S}^n} = \sum_{E,E'\in\Pi_\epsilon} |\tilde{\sigma}^E\rangle\!\langle\tilde{\sigma}^{E'}|_{\mathsf{RP}^n\mathsf{S}^n} \leq 2^{h(\epsilon)n} \sum_{E\in\Pi_\epsilon} \left|\tilde{\sigma}^E\right\rangle\!\left\langle\tilde{\sigma}^E\right|_{\mathsf{RP}^n\mathsf{S}^n} \ , \tag{4.19}$$

car l'ensemble Π_ϵ contient au plus $2^{h(\epsilon)n}$ éléments. De plus, on sait par la définition de $|\tilde{\sigma}^E\rangle_{\mathsf{RP}^n\mathsf{S}^n}$ que

$$\frac{\tilde{\sigma}^E_{\mathsf{S}^n}}{\|\tilde{\sigma}^E_{\mathsf{S}^n}\|_1} = \left(\bigotimes_{i\notin E} \frac{\mathbb{1}_{\mathsf{S}_i}}{2}\right) \otimes \psi_{\mathsf{S}_E} \leq 2^{-n+|E|}\mathbb{1}_{\mathsf{S}^n}$$

pour une famille quelconque d'états normalisés ψ_{S_E} qui vivent sur les registres $\mathsf{S}_E = \bigotimes_{i\in E}\mathsf{S}_i$. Puisque $|E| \leq \epsilon n$, il s'ensuit par (4.19) que

$$\sigma_{\mathsf{S}^n} \leq 2^{h(\epsilon)n} \sum_{E\in\Pi_\epsilon} \tilde{\sigma}^E_{\mathsf{S}^n} \leq 2^{-(1-\epsilon-h(\epsilon))n}\mathbb{1}_{\mathsf{S}^n}$$

et on peut donc conclure que $\mathrm{H}_\infty(\mathsf{S}^n)_\sigma \geq (1-\epsilon-h(\epsilon))n$ par la définition de la min-entropie pour les états quantiques. □

Borner inférieurement la min-entropie de la sortie de Bob est une question d'appliquer le lemme 4.5.2 à l'état réduit de Bob après l'étape d'échantillonnage du protocole de la figure 4.4, état qui peut être approximé par un état idéal par notre résultat d'échantillonnage (corollaire 4.4.2).

Lemme 4.5.3 (Min-entropie de la sortie de Bob)**.** *Si Bob est honnête, alors pour tout $\gamma > 0$, sa sortie $X_B \in \{0,1\}^n$ satisfait*

$$\mathrm{H}_\infty(X_B) \geq (1-\gamma)n \ ,$$

sauf avec probabilité négligeable en n.

Démonstration. Soit $\rho_{\mathsf{B}^n} \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$ l'état normalisé de Bob après l'étape 2 du protocole de la figure 4.4 conditionné sur le fait que Bob a accepté le résultat de l'échantillonnage. Soit P_{acc} la probabilité qu'il accepte l'échantillonnage. Par le corollaire 4.4.2, on sait que pour tout $\epsilon > 0$ il existe un opérateur idéal ψ_{B^n} et un opérateur σ_{B^n} avec norme de trace négligeable tels que

$$\rho_{\mathsf{B}^n} \leq P_{\text{acc}}^{-1}(c_{N,d^2}\psi_{\mathsf{B}^n} + \sigma_{\mathsf{B}^n}) \ . \tag{4.20}$$

Définissons $\tilde{\psi}_{\mathsf{B}^n} = \frac{c_{N,d^2}}{P_{\text{acc}}} \cdot \psi_{\mathsf{B}^n}$. La partie droite de (4.20) satisfait $\left\| \frac{c_{N,d^2}}{P_{\text{acc}}}(\psi_{\mathsf{B}^n} + \sigma_{\mathsf{B}^n}) - \tilde{\psi}_{\mathsf{B}^n} \right\|_1 = \frac{1}{P_{\text{acc}}} \|\sigma_{\mathsf{B}^n}\|_1$, quantité qui est négligeable en N dès que P_{acc} est non négligeable. On peut en déduire que, sauf avec probabilité négligeable, la partie droite de (4.20) se comportera exactement comme $\tilde{\psi}_{\mathsf{B}^n}$. En particulier, la min-entropie de la partie droite de (4.20) sera bornée inférieurement par

$$\mathrm{H}_\infty(\mathsf{B}^n)_{\tilde{\psi}} = \mathrm{H}_\infty(\mathsf{B}^n)_{\psi} - \log \frac{c_{N,d^2}}{P_{\text{acc}}} \geq (1 - \epsilon - h(\epsilon))n - \log \frac{c_{N,d^2}}{P_{\text{acc}}} \ , \tag{4.21}$$

sauf avec probabilité négligeable, où l'inégalité ci-dessus découle du lemme 4.5.2 car $\tilde{\psi}$ est ϵ-idéal.

En utilisant la borne (4.21), on peut faire la déclaration suivante sur la min-entropie de ρ_{B^n} : celle-ci sera bornée inférieurement par

$$(1 - \epsilon - h(\epsilon) - \alpha)n$$

sauf si un ou l'autre de deux évènements à probabilité négligeable se produit. Le premier de ces évènements est que ρ_{B^n} se comporte comme σ_{B^n} plutôt que comme $\tilde{\psi}_{\mathsf{B}^n}$, et le second est que Bob accepte le résultat d'un échantillonnage qui a probabilité $P_{\text{acc}} \leq c_{N,d^2} \cdot 2^{-\alpha n}$ d'être accepté.

On peut donc conclure que la sortie de Bob X_B obtenu en mesurant ρ_{B^n} dans la base calculatoire aura min-entropie au moins $(1 - \epsilon - h(\epsilon) - \alpha)n$, sauf avec probabilité négligeable. La preuve est complétée en choisissant ϵ et α tels que $\gamma = \epsilon + h(\epsilon) + \alpha$. □

4.6 Conclusion

Dans ce chapitre, nous avons vu comment il est possible de s'assurer qu'un registre quantique de la forme $\mathcal{H}^{\otimes n}$ préparé par un adversaire est *près* d'un état de référence $\varphi^{\otimes n}$ pour une matrice de densité $\varphi \in \mathcal{D}(\mathcal{H})$ quelconque. Le protocole d'échantillonnage qui effectue cette vérification doit être interactif, sans quoi il est impossible de distinguer l'état correct d'un état fixe préparé dans le but de tromper l'échantillonneur. Cette interaction introduit des subtilités qui ne sont pas présentes pour les problèmes d'échantillonnage de populations classique, ou quantique avec état de référence pur. Ainsi une contribution de ces travaux est de définir à la fois en quoi consiste un état idéal pour ce type de problème, et ce qu'il est possible de prouver sur l'état résultat d'un tel protocole.

Nous avons proposé un modèle général de protocole de certification d'états de référence mixtes et avons montré que tout protocole qui satisfait le modèle et certaines propriétés naturelles peuvent être analysés à l'aide de nos techniques. En plus du protocole naturel où l'échantillonneur demande au prouveur les registres de purifications, ce modèle inclut aussi comme cas spéciaux un protocole OLCC pour échantillonner des demies paires EPR ainsi que les résultats précédents d'échantillonnage d'états purs.

Nous appliquons cette technique pour analyser un protocole de lancer de pièce où au lieu de minimiser le biais sur chaque lancer, on cherche à maximiser la min-entropie totale de la chaine produite. Nous montrons qu'il est possible à deux participants de produire une chaine commune $X \in \{0,1\}^n$ de min-entropie arbitrairement près du maximum n, et ce même si un des participants est malhonnête. Ce résultat est une amélioration du cas classique où la plus grande incertitude possible est de $n/2$ bits de min-entropie, produite par le protocole trivial où chacun des participants produit une chaine aléatoire de $n/2$ bits [HMQU06].

4.6.1 Problèmes ouverts

Les travaux du chapitre 4 sont une source intarissable de problèmes ouverts, car ces travaux touchent des problèmes fondamentaux où des énoncés intuitifs ne sont pas nécessairement faciles à prouver.

La première question ouverte concerne la tâche en soi. Les travaux de ce chapitre concernent *l'échantillonnage statistique* d'une population quantique, mais la tâche que nous réalisons est plutôt la *certification* d'un état, dans le sens où la procédure d'échantillonnage rejette le résultat dès qu'une erreur est observée. Un vrai protocole d'échantillonnage calculerait plutôt le taux d'erreur $\delta \geq 0$ observé et conclurait que le reste des positions a un taux d'erreur $\delta \pm \epsilon$ pour un petit $\epsilon > 0$. Notons qu'une partie de cette restriction est due à la particularité de l'échantillonnage d'états *mixtes* et d'un prouveur potentiellement malhonnête : même si on établit que le taux d'erreur est faible dans l'échantillon, celui-ci peut introduire des erreurs dans le reste de la population par la suite, et il se peut aussi qu'on observe un grand taux d'erreur alors que le reste de la population a peu d'erreurs si le prouveur introduit intentionnellement des erreurs dans l'échantillon.

Une deuxième question ouverte concerne l'état de référence φ de notre protocole d'échantillonnage. Nos résultats nous permettent d'échantillonner en fonction d'un état de la forme $\varphi^{\otimes N}$, mais ne nous permettent pas directement d'échantillonner une population en fonction d'états de référence différents pour chaque position, par exemple en fonction de l'état $\bigotimes_{i=1}^{N} \varphi_{x_i}$ pour $x \in \{0,1\}^N$ et où φ_0 et φ_1 sont deux états mixtes quelconques. Certaines situations nous permettent d'échantillonner selon plusieurs états de références, par exemple si les états φ_0 et φ_1 sont unitairement reliés, c'est-à-dire s'il existe une transformation unitaire

U telle que $\varphi_0 = U\varphi_1 U^*$. Notons que c'est la technique utilisée dans [BF10] pour l'échantillonnage des états purs, car tous les états purs sont unitairement reliés. Une autre technique prometteuse, mais que nous n'avons pas analysée en détail est de considérer les positions $I_0 := \{i \in [N] : x_i = 0\}$ et $I_1 := \{i \in [N] : x_i = 1\}$ comme des populations distinctes et d'échantillonner selon l'état de référence φ_c pour la population I_c pour $c \in \{0, 1\}$. Cela suppose évidemment que le nombre d'états de références distincts est constant et que chacune des populations est assez grande pour obtenir un énoncé non trivial.

Un problème intéressant est de trouver d'autres exemples de protocoles d'échantillonnage analysés de manière ad hoc, mais qui peuvent maintenant être analysés par les outils introduits dans le chapitre 4. Il serait également pertinent de trouver de nouveaux protocoles d'échantillonnage qui sont plus *pratiques*, c'est-à-dire qui nécessitent une technologie moindre que l'échantillonnage par purification. Par exemple, on pourrait imaginer un protocole d'échantillonnage OLCC pour un état de référence arbitraire φ semblable à celui de la figure 4.3 pour l'échantillonnage de demi-paires EPR qui demande au prouver de montrer qu'il possède une purification de φ en devant *prédire* quel sera le résultat d'une mesure dans la *base propre* de φ et en comparant les statistiques de ces mesures aux *valeurs propres* de φ. On peut aussi s'imaginer une variante de l'échantillonnage par purification où l'envoi des registres quantiques est *séquentiel*, c'est-à-dire que le prouveur envoie le premier qubit, l'échantillonneur lui dit s'il vérifiera ou non la purification pour cette position, puis le prouveur envoie le deuxième qubit, etc.

Finalement, une dernière question ouverte est de trouver une application à la tâche cryptographique de génération sûre d'aléa partagé introduite à la dernière section du chapitre 4. En particulier, il serait intéressant de trouver une application cryptographique qui est sûre si elle utilise notre protocole de génération d'aléa partagé, mais qui n'est pas sûre si on utilise plutôt un protocole optimal pour le lancer d'une pièce, c'est-à-dire un protocole qui exploite pleinement la min-entropie produite par la sortie de notre protocole. Pour pouvoir appliquer notre protocole, il serait également utile de savoir s'il est sûr dans le modèle UC, ou seulement dans le modèle à sécurité autonome.

Chapitre 5

Conclusion

Le thème unificateur de cette thèse est de fournir des outils de preuve aux cryptographes quantiques qui permettent de réduire le comportement malhonnête arbitraire (actif) d'un adversaire à un comportement honnête ou à un comportement malhonnête, mais classique (passif). Ces résultats ont permis de contribuer à l'avancement des connaissances dans le domaine de l'évaluation sûre quantique en servant d'outils de preuve dans l'analyse de protocoles nouveaux et anciens.

Au chapitre 3, nous avons montré comment le comportement d'un adversaire *adapté*, disposant d'information auxiliaire quantique, peut être réduit à celui d'un adversaire *non adapté* ne disposant pas de telle information auxiliaire. Cette réduction s'applique dans un contexte très général et son utilité est démontrée par la résolution de deux problèmes ouverts, où les preuves reposent largement sur notre réduction. Le premier de ces problèmes concerne la puissance cryptographique de la primitive 1CC dans le monde quantique, un problème ouvert de [FKS+13]. Nous montrons que cette primitive est complète dans le modèle UC quantique, c'est-à-dire qu'elle appartient à la classe des primitives les plus puissantes pour la définition de sécurité la plus forte. Le deuxième problème ouvert concerne la sûreté du protocole de mise en gage quantique de [BCJL93]. La question de la sûreté de ce protocole sous des hypothèses raisonnables restait sans réponse depuis qu'on sait que la mise en gage inconditionnellement sûre est impossible [May97]. Nous fournissons une réponse à cette question en montrant que ce protocole est sûr dans une version légèrement modifiée du modèle à mémoire bornée.

Au chapitre 4, nous avons montré qu'il est possible de vérifier qu'une population quantique a été préparée dans un certain état, tel que décrit par une matrice de densité. Cette vérification a lieu dans un contexte où un adversaire peut avoir préparé la population quantique de manière arbitraire. Nous montrons qu'en *échantillonnant* la population à l'aide d'un protocole interactif, il est possible de s'assurer que le

prouveur adversariel n'a pas trop dévié du comportement honnête. Cette procédure a des applications intéressantes en cryptographie, en particulier, elle permet de vérifier si une population quantique a été préparée selon une distribution uniforme (représentée par une demie paire EPR). Nous utilisons donc les résultats d'échantillonnage du chapitre 4 pour analyser la sûreté d'un protocole pour une nouvelle primitive généralisant le tirage d'une pièce : deux participants peuvent générer une chaine de n bits dont la min-entropie est arbitrairement près de maximale, sauf avec probabilité négligeable.

Finalement, nous avons discuté de questions ouvertes qui ont trait aux résultats de cette thèse aux sections 3.5.1 et 4.6.1.

Index

Bibliographie

[ACMT+07] Koenraad M. R. Audenaert, John Calsamiglia, Ramón Muñoz-Tapia, Emili Bagan, Ll. Masanes, Antonio Acin et Frank Verstraete : Discriminating states : The quantum chernoff bound. *Physical Review Letters*, 98(16):160501, 2007.

[Amb01] Andris Ambainis : A new protocol and lower bounds for quantum coin flipping. *In Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 134–142. ACM, 2001.

[Amb04] Andris Ambainis : A new protocol and lower bounds for quantum coin flipping. *Journal of Computer and System Sciences*, 68(2):398–416, 2004.

[AW02] Rudolf Ahlswede et Andreas Winter : Strong converse for identification via quantum channels. *IEEE Transactions on Information Theory*, 48(3):569–579, 2002.

[BB83] Charles H. Bennett et Gilles Brassard : Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing. *In Proceedings of IEEE International Symposium on Information Theory*, page 91, 1983.

[BB84] Charles H. Bennett et Gilles Brassard : Quantum cryptography : Public key distribution and coin tossing. *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BB89] Charles H. Bennett et Gilles Brassard : Experimental quantum cryptography : the dawn of a new era for quantum cryptography : the experimental prototype is working. *ACM Sigact News*, 20(4):78–80, 1989.

[BBB+92] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail et John Smolin : Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

[BBBW83] Charles H. Bennett, Gilles Brassard, Seth Breidbart et Stephen Wiesner : Quantum cryptography, or unforgeable subway tokens. *In Advances in Cryptology—CRYPTO '83*, pages 267–275. Springer, 1983.

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres et William K Wootters : Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895, 1993.

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau et Ueli Maurer : Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau et Marie-Hélene Skubiszewska : Practical quantum oblivious transfer. *In Advances in Cryptology—CRYPTO '91*, pages 351–366. Springer, 1991.

[BBR88] Charles H. Bennett, Gilles Brassard et Jean-Marc Robert : Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[BCJL93] G. Brassard, C. Crépeau, R. Jozsa et D. Langlois : A quantum bit commitment scheme provably unbreakable by both parties. *In Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science*, pages 362–371, 1993.

[BCR11] Mario Berta, Matthias Christandl et Renato Renner : The quantum reverse shannon theorem based on one-shot information theory. *Communications in Mathematical Physics*, 306(3):579–615, septembre 2011.

[BCS12] Harry Buhrman, Matthias Christandl et Christian Schaffner : Complete insecurity of quantum protocols for classical two-party computation. *Physical Review Letters*, 109(16): 160501, 2012.

[Ben92] Charles H. Bennett : Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[BF10] Niek J. Bouman et Serge Fehr : Sampling in a quantum population, and applications. *In Advances in Cryptology—CRYPTO 2010*, volume 6223 de *Lecture Notes in Computer Science*, pages 724–741. Springer, 2010.

[Blu82] Manuel Blum : Coin flipping by telephone. *Proceedings of COMPCON, IEEE*, 1982.

[BW92] Charles H. Bennett et Stephen J. Wiesner : Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881, 1992.

[Can01] Ran Canetti : Universally composable security : a new paradigm for cryptographic protocols. *In Proceedings of the IEEE International Conference on Cluster Computing*, pages 136–145, 2001.

[CK09] André Chailloux et Iordanis Kerenidis : Optimal quantum strong coin flipping. *In Proceedings of FOCS 2009*, pages 527–533, 2009.

[CKMR07] Matthias Christandl, Robert König, Graeme Mitchison et Renato Renner : One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007.

[CKR09a] Matthias Christandl, Robert König et Renato Renner : Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102:020504, janvier 2009.

[CKR09b] Matthias Christandl, Robert König et Renato Renner : Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102(2):020504, 2009.

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky et Amit Sahai : Universally composable two-party and multi-party secure computation. *In Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*, pages 494–503. ACM, 2002.

[Col07] Roger Colbeck : Impossibility of secure two-party classical computation. *Physical Review A*, 76(6):062308, 2007.

[Cré88] Claude Crépeau : Equivalence between two flavours of oblivious transfers. *In* Carl Pomerance, éditeur : *Advances in Cryptology—CRYPTO '87*, pages 350–354. Springer, 1988.

[Cré94] Claude Crépeau : Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.

[CW79] J. Lawrence Carter et Mark N. Wegman : Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[DFL+09] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail et Christian Schaffner : Improving the security of quantum protocols via commit-and-open. *In Advances in Cryptology—CRYPTO 2009*, volume 5677, pages 408–427. Springer, 2009.

[DFLS16a] Frédéric Dupuis, Serge Fehr, Philippe Lamontagne et Louis Salvail : Adaptive versus non-adaptive strategies in the quantum setting with applications. *In Advances in Cryptology —CRYPTO 2016*, pages 33–59. Springer, 2016.

[DFLS16b] Frédéric Dupuis, Serge Fehr, Philippe Lamontagne et Louis Salvail : Adaptive versus non-adaptive strategies in the quantum setting with applications. 6th International Conference on Quantum Cryptography, QCrypt2016, 2016.

[DFLS17] Frédéric Dupuis, Serge Fehr, Philippe Lamontagne et Louis Salvail : Secure certification of mixed quantum states and application to two-party randomness generation. Non publié à l'écriture de ce document, 2017.

[DFSS07] Ivan B. Damgård, Serge Fehr, Louis Salvail et Christian Schaffner : Secure identification and QKD in the bounded-quantum-storage model. *In Advances in Cryptology—*

CRYPTO '07, volume 4622 de *Lecture Notes in Computer Science*, pages 342–359. Springer-Verlag, 2007.

[DFSS08] Ivan Damgård, Serge Fehr, Louis Salvail et Christian Schaffner : Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.

[FF16] Serge Fehr et Max Fillinger : On the composition of two-prover commitments, and applications to multi-round relativistic commitments. *In Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 477–496. Springer, 2016.

[FKS+13] Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou et Vassilis Zikas : Feasibility and completeness of cryptographic tasks in the quantum world. *In* Amit Sahai, éditeur : *Theory of Cryptography*, volume 7785 de *Lecture Notes in Computer Science*, pages 281–296. Springer, 2013.

[FS09] Serge Fehr et Christian Schaffner : Composing quantum protocols in a classical environment. *In Theory of Cryptography Conference*, volume 5444, pages 350–367. Springer, 2009.

[GW07] Gus Gutoski et John Watrous : Toward a general theory of quantum games. *In Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 565–574. ACM, 2007.

[HMQU06] Dennis Hofheinz, Jörn Müller-Quade et Dominique Unruh : On the (im-)possibility of extending coin toss. *In Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 504–521. Springer, 2006.

[HS99] Peter Høyer et Louis Salvail, 1999 : Protocole non publié.

[IPS08] Yuval Ishai, Manoj Prabhakaran et Amit Sahai : Founding cryptography on oblivious transfer – efficiently. *In Advances in Cryptology – CRYPTO 2008 : 28th Annual International Cryptology Conference*, pages 572–591. Springer, 2008.

[Kil88] Joe Kilian : Founding cryptography on oblivious transfer. *In Proceedings of the ACM Symposium on Theory of Computing*, STOC '88, pages 20–31. ACM, 1988.

[Kil91] Joe Kilian : A general completeness theorem for two party games. *In Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing*, STOC '91, pages 553–560, 1991.

[Kil00] Joe Kilian : More general completeness theorems for secure two-party computation. *In Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 316–324, 2000.

[Kit03] Alexei Kitaev : Quantum coin-flipping. Presentation at the 6th Workshop on Quantum Information Processing (QIP 2003), 2003.

[KL14] Jonathan Katz et Yehuda Lindell : *Introduction to modern cryptography.* CRC press, 2014.

[KMQ11a] Daniel Kraschewski et Jörn Müller-Quade : *Completeness Theorems with Constructive Proofs for Finite Deterministic 2-Party Functions*, pages 364–381. Springer, 2011.

[KMQ11b] Daniel Kraschewski et Jörn Müller-Quade : Completeness theorems with constructive proofs for finite deterministic 2-party functions. *In Theory of Cryptography*, volume 6597 de *Lecture Notes in Computer Science*, pages 364–381. Springer, 2011.

[KN04] Iordanis Kerenidis et Ashwin Nayak : Weak coin flipping with small bias. *Information Processing Letters*, 89(333):131–135, 2004.

[Kra13] Daniel Kraschewski : *Complete primitives for information-theoretically secure two-party computation.* Thèse de doctorat, Karlsruhe Institute of Technology, 2013.

[KWW12] Robert König, Stephanie Wehner et Jürg Wullschleger : Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, mars 2012.

[LC98] Hoi-Kwong Lo et Hoi Fung Chau : Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D : Nonlinear Phenomena*, 120(1-2):177–187, 1998.

[Lo97] Hoi-Kwong Lo : Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154, 1997.

[May96] Dominic Mayers : The trouble with quantum bit commitment. *arXiv preprint quant-ph/9603015*, 1996.

[May97] Dominic Mayers : Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414, 1997.

[Moc04] Carlos Mochon : Quantum weak coin-flipping with bias of 0.192. *In Proceedings of FOCS 2004*, pages 2–11, 2004.

[Moc05] Carlos Mochon : Large family of quantum weak coin-flipping protocols. *Physical Review A*, 72(2):022341, 2005.

[Moc07] Carlos Mochon : Quantum weak coin flipping with arbitrarily small bias. *arXiv preprint arXiv :0711.4114*, 2007.

[MPR09] Hemanta K. Maji, Manoj Prabhakaran et Mike Rosulek : Complexity of multi-party computation problems : The case of 2-party symmetric secure function evaluation. *In Theory of Cryptography Conference*, pages 256–273. Springer, 2009.

[MPR10] Hemanta K. Maji, Manoj Prabhakaran et Mike Rosulek : A zero-one law for cryptographic complexity with respect to computational UC security. *In Advances in Cryptology—*

CRYPTO 2010, volume 6223 de *Lecture Notes in Computer Science*, pages 595–612. Springer, 2010.

[MPR12] Hemanta K. Maji, Manoj Prabhakaran et Mike Rosulek : A unified characterization of completeness and triviality for secure function evaluation. *In Progress in Cryptology—INDOCRYPT 2012*, volume 7668 de *Lecture Notes in Computer Science*, pages 40–59. Springer, 2012.

[ON02] Tomohiro Ogawa et Hiroshi Nagaoka : A new proof of the channel coding theorem via hypothesis testing in quantum information theory. *In IEEE International Symposium on Information Theory*, page 73, 2002.

[PJL+14] Anna Pappa, Paul Jouguet, Thomas Lawson, André Chailloux, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis et Eleni Diamanti : Experimental plug and play quantum coin flipping. *Nature communications*, 5:3717, 2014.

[Ple98] Vera Pless : *Introduction to the Theory of Error-Correcting Codes*. John Wiley & Sons, Inc., 1998.

[PR08] Manoj Prabhakaran et Mike Rosulek : Cryptographic complexity of multi-party computation problems : Classifications and separations. *In* David Wagner, éditeur : *Advances in Cryptology–CRYPTO 2008*, pages 262–279. Springer, 2008.

[Rab81] Michael O. Rabin : How to exchange secrets with oblivious transfer. Rapport technique TR-81, Aiken Computation Lab, Harvard University, 1981.

[Rén61] Alfréd Rényi : On measures of entropy and information. *In Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1 : Contributions to the Theory of Statistics*. The Regents of the University of California, 1961.

[Ren05] Renato Renner : *Security of quantum key distribution*. Thèse de doctorat, ETH Zürich, 2005.

[Ren07] Renato Renner : Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, (3):645–649, 2007.

[Ren10] Renato Renner : Simplifying information-theoretic arguments by post-selection. *In Quantum Cryptography and Computing*, volume 26, pages 66–75, 2010.

[RK05] Renato Renner et Robert König : Universally composable privacy amplification against quantum adversaries. *In* Joe Kilian, éditeur : *Theory of Cryptography*, volume 3378 de *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005.

[Sch07] Christian Schaffner : *Cryptography in the Bounded-Quantum-Storage Model*. Thèse de doctorat, Aarhus Universitet, 2007.

[Sch10] Christian Schaffner : Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Physical Review A*, 82(3):032308, 2010.

[Sha49] Claude E. Shannon : Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715, 1949.

[Sho94] Peter W. Shor : Algorithms for quantum computation : discrete logarithms and factoring. *In Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE, 1994.

[SR01] Robert W. Spekkens et Terry Rudolph : Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(1):012310, 2001.

[SR02] Robert W. Spekkens et Terry Rudolph : Quantum protocol for cheat-sensitive weak coin flipping. *Physical Review Letters*, 89(22):227901, 2002.

[STW09] Christian Schaffner, Barbara Terhal et Stephanie Wehner : Robust cryptography in the noisy-quantum-storage model. *Quantum Information & Computation*, 9(11):963–996, novembre 2009.

[Tom12] Marco Tomamichel : *A framework for non-asymptotic quantum information theory.* Thèse de doctorat, ETH Zurich, 2012.

[Unr10] Dominique Unruh : Universally composable quantum multi-party computation. *In* Henri Gilbert, éditeur : *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 de *Lecture Notes in Computer Science*, pages 486–505. Springer, 2010.

[Wat11] John Watrous : Theory of quantum information, 2011. Notes de cours, disponibles à l'adresse `https://cs.uwaterloo.ca/~watrous/LectureNotes.html`.

[Wat17] John Watrous : The theory of quantum information, 2017. Ébauche de livre, disponible à l'adresse `https://cs.uwaterloo.ca/~watrous/TQI/`.

[WC81] Mark N. Wegman et J.Lawrence Carter : New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265 – 279, 1981.

[WCSL10] Stephanie Wehner, Marcos Curty, Christian Schaffner et Hoi-Kwong Lo : Implementation of two-party protocols in the noisy-storage model. *Physical Review A*, 81(5):052336, 2010.

[Wie83] Stephen Wiesner : Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[Win99] Andreas Winter : Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, novembre 1999.

[WST08] Stephanie Wehner, Christian Schaffner et Barbara M. Terhal : Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

[WW08] Stephanie Wehner et Jürg Wullschleger : *Composable Security in the Bounded-Quantum-Storage Model*, pages 604–615. Springer, 2008.

[ZS01] Karol Życzkowski et Hans-Jürgen Sommers : Induced measures in the space of mixed quantum states. *Journal of Physics A : Mathematical and General*, 34(35):7111, 2001.

Annexe A

Invariance sous les permutations de protocoles d'échantillonnage

A.1 Preuve de la proposition 4.3.1

On peut supposer sans perte de généralité que l'état $\rho_{\mathsf{RS}^N} \in \mathcal{D}(\mathcal{H}_{\mathsf{R}} \otimes \mathcal{H}_{\mathsf{S}}^{\otimes N})$ est pur et que la stratégie de l'adversaire contre le protocole de la figure 4.1 est décrite par une famille d'isométries de la forme $U^t_{\mathsf{R}\to\mathsf{R}'\mathsf{P}^k}$ pour $t \subseteq [N]$ de taille k, où P^k représente le registre envoyé à Sam et qui devrait contenir les purifications de φ_{S}, et où R' est un registre conservé par Paul.

Pour nous simplifier la vie, définissons une isométrie $V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}$ qui, pour tout $t \subseteq [N]$, envoie le contenu des sous-registres S_i pour $i \in t$ dans les k derniers sous-registres (qu'on notera simplement S^k) et qui envoie le contenu des sous-registres S_i pour $i \notin t$ dans les premiers $n = N - k$ sous-registres (notés S^n). Autrement dit, l'isométrie V^t_{S} regroupe ensemble les registres qui seront échantillonnés.

Pour une stratégie adversarielle telle que décrite ci-dessus, le CPTN $\mathcal{E}^{\mathrm{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$ qui décrit l'état de sortie du protocole en fonction de l'état d'entrée ρ_{RS^N} est défini par

$$\mathcal{E}^{\mathrm{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N}) := \frac{1}{\binom{N}{k}} \sum_{t\subseteq[N]} \mathrm{tr}_{\mathsf{R}'} \left(\langle\varphi|^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k} \cdot [U^t_{\mathsf{R}} \otimes V^t_{\mathsf{S}^N}](\rho_{\mathsf{RS}^N}) \cdot |\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k} \right) .$$

où les opérateurs identité qui agissent sur les registres $\mathsf{R}'\mathsf{S}^n$ sont laissés implicites et où $[U](\rho)$ est un raccourci pour $U\rho U^*$ pour toute isométrie U.

La propriété suivante de $V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}$ sera utile pour démontrer le lemme A.1.1 ci-dessous.

Remarque A.1.1. Soit $\pi \in \mathcal{S}_N$, et soit $t_\pi = \{\pi^{-1}(i) \,:\, i \in [k]\}$. Il existe $\tau^\pi \in \mathcal{S}_k$ et $\bar{\tau}^\pi \in \mathcal{S}_n$ tels que $V^{[k]}_{\mathsf{S}^N \to \mathsf{S}^n\mathsf{S}^k} \cdot \pi_{\mathsf{S}} = (\bar{\tau}^\pi_{\mathsf{S}^n} \otimes \tau^\pi_{\mathsf{S}^k}) \cdot V^{t_\pi}_{\mathsf{S}^N \to \mathsf{S}^n\mathsf{S}^k}$. De plus, il y a une bijection entre les permutations $\pi \in \mathcal{S}_N$ et les triplets de la forme $(t_\pi, \tau^\pi, \bar{\tau}^\pi)$.

Lemme A.1.1. *Le protocole* **Purification-Based Sampling** *de la figure 4.1 satisfait le premier critère de la définition 4.3.1.*

Démonstration. On doit montrer l'existence d'un CPTN $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N \to \Pi\mathsf{S}^n}$ tel que pour tout état d'entrée $\rho_{\mathsf{R}\mathsf{S}^N}$,

$$\frac{1}{n!} \sum_{\pi \in \mathcal{S}_n} |\pi\rangle\langle\pi|_\Pi \otimes \pi_{\mathsf{S}'} \mathcal{E}^{\text{acc}}_{\mathsf{R}\mathsf{S}^N \to \mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N}) \pi^*_{\mathsf{S}'} = \bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N \to \Pi\mathsf{S}^n}(\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}) \tag{A.1}$$

pour une purification $|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle \in \text{Sym}^N(\mathcal{H}_\mathsf{P} \otimes \mathcal{H}_\mathsf{S})$ de $\frac{1}{N!}\sum_{\pi \in \mathcal{S}_N} \pi_{\mathsf{S}^N} \rho_{\mathsf{S}^N} \pi^*_{\mathsf{S}^N}$ où $\mathcal{E}^{\text{acc}}_{\mathsf{R}\mathsf{S}^N \to \mathsf{S}^n}$ est défini plus haut dans cette section.

Soit $|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle$ une purification arbitraire de $\frac{1}{N!}\sum_{\pi \in \mathcal{S}_N} \pi_{\mathsf{S}^N} \rho_{\mathsf{S}^N} \pi^*_{\mathsf{S}^N}$ vivant dans le sous-espace symétrique. Puisque toutes les purifications sont équivalentes à une isométrie près sur les registres de purification, il existe une isométrie $W_{\mathsf{P}^N \to \mathsf{R}\bar{\Pi}}$ telle que

$$(W_{\mathsf{P}^N} \otimes \mathbb{1}_{\mathsf{S}^N})|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle = \frac{1}{\sqrt{N!}} \sum_{\pi \in \mathcal{S}_n} (\mathbb{1}_\mathsf{R} \otimes \pi_{\mathsf{S}^N})|\rho_{\mathsf{R}\mathsf{S}^N}\rangle \otimes |\pi\rangle_{\bar{\Pi}} \ .$$

Soit $\bar{U}_{\mathsf{P}^N \to \bar{\mathsf{R}}\mathsf{P}^k}$ une isométrie qui effectue les transformations suivantes de manière unitaire sur le registre P^N de $|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle$:

1. Appliquer W_{P^N}, produisant les registres R et $\bar{\Pi}$.
2. À partir de la permutation $\pi \in \mathcal{S}_N$ qui se trouve dans le registre $\bar{\Pi}$, calculer t_π, $\tau^\pi \in \mathcal{S}_k$ et $\bar{\tau}^\pi \in \mathcal{S}_n$ tels que définis par la remarque A.1.1, c'est-à-dire tels que $V^{[k]}_{\mathsf{S}^N \to \mathsf{S}^n\mathsf{S}^k} \cdot \pi_{\mathsf{S}} = (\tau^\pi_{\hat{\mathsf{S}}} \otimes \bar{\tau}^\pi_{\mathsf{S}'}) \cdot V^{t_\pi}_{\mathsf{S}^N \to \mathsf{S}^n\mathsf{S}^k}$.
3. Appliquer l'attaque $U^{t_\pi}_{\mathsf{R} \to \mathsf{R}'\mathsf{P}^k}$ sur le registre R, produisant ainsi les registres R' et P^k, et réordonner les registres P^k en utilisant la permutation τ^π de manière à ce que chaque P_i est correctement aligné avec le S_i correspondant lorsque ces registres sont envoyés à Sam.
4. Soit le registre $\bar{R}$ composé des registres R' et $\bar{\Pi}$. Produire en sortie les registres P^k, $\bar{\mathsf{R}}$ et un registre Π contenant la permutation $\bar{\tau}^\pi$ qui agit sur les registres de sortie S^n (c'est-à-dire sur les registres non échantillonnés).

À partir de la définition de l'isométrie $\bar{U}_{\mathsf{P}^N \to \bar{\mathsf{R}}\mathsf{P}^k}$ ci-dessus, on a

$$\begin{aligned}
&(\bar{U}_{\mathsf{P}^N \to \bar{\mathsf{R}}\mathsf{P}^k} \otimes V^{[k]}_{\mathsf{S}^N \to \mathsf{S}^n\mathsf{S}^k})|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle \\
&= \frac{1}{\sqrt{N!}} \sum_{\pi \in \mathcal{S}_N} (\tau^\pi_{\mathsf{P}^k} \otimes \tau^\pi_{\mathsf{S}^k} \otimes \bar{\tau}^\pi_{\mathsf{S}^n})(U^{t_\pi}_{\mathsf{R} \to \mathsf{R}'\mathsf{P}^k} \otimes V^{t_\pi}_{\mathsf{S}^N \to \mathsf{S}^n\mathsf{S}^k})|\rho_{\mathsf{R}\mathsf{S}^N}\rangle|\pi\rangle_{\bar{\Pi}}|\bar{\tau}^\pi\rangle_\Pi
\end{aligned}$$

En traçant le registre $\bar{\Pi}$ de l'état ci-dessus et en utilisant la bijection entre les permutations $\pi \in \mathcal{S}_N$ et les triplets $(t_\pi, \tau^\pi, \bar{\tau}^\pi)$ pour briser la somme sur π en sommes sur t, τ et $\bar{\tau}$, on obtient l'opérateur

$$\begin{aligned}
&\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N}[(\tau^\pi_{\mathsf{P}^k}\otimes\tau^\pi_{\mathsf{S}^k}\otimes\mathbb{1}_{\mathsf{R}'}\otimes\bar{\tau}^\pi_{\mathsf{S}^n})(U^{t_\pi}_{\mathsf{R}\to\mathsf{R}'\mathsf{P}^k}\otimes V^{t_\pi}_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k})](\rho_{\mathsf{R}\mathsf{S}^N})\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi\\
&=\frac{1}{n!}\frac{1}{k!}\frac{1}{\binom{N}{k}}\sum_{\bar{\tau}\in\mathcal{S}_n}\bar{\tau}_{\mathsf{S}^n}\left(\sum_{\substack{\tau\in\mathcal{S}_k\\ t\subseteq[N]:|t|=k}}[(\tau_{\mathsf{P}^k}\otimes\tau_{\mathsf{S}^k})(U^t_{\mathsf{R}}\otimes V^t_{\mathsf{S}^N})](\rho_{\mathsf{R}\mathsf{S}^N})\right)(\bar{\tau}_{\mathsf{S}^n})^*\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi
\end{aligned}$$

En prenant le produit interne partiel de l'opérateur ci-dessus avec $|\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}$ et en prenant la trace partielle du registre R' on obtient

$$\begin{aligned}
&\frac{1}{n!\binom{N}{k}}\sum_{\bar{\tau}\in\mathcal{S}_n}\bar{\tau}_{\mathsf{S}^n}\left(\sum_t\mathrm{tr}_{\mathsf{R}'}\left(\langle\varphi|^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\cdot[U^t_{\mathsf{R}}\otimes V^t_{\mathsf{S}^N}](\rho_{RS^N})\cdot|\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\right)\right)(\bar{\tau}_{\mathsf{S}^n})^*\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi\\
&\quad=\frac{1}{n!}\sum_{\bar{\tau}\in\mathcal{S}_n}\bar{\tau}_{\mathsf{S}^n}\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}(\rho_{\mathsf{R}\mathsf{S}^N})\bar{\tau}^*_{\mathsf{S}^n}\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi
\end{aligned}$$

où la somme sur les permutations τ a disparu, car l'état $|\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}$ est invariant sous les permutations. Alors, le CPTN $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ défini par

$$\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}):=\mathrm{tr}_{\bar{\mathsf{R}}}\left(\langle\varphi|^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\cdot[\bar{U}_{\mathsf{P}^N}\otimes V^{[k]}_{\mathsf{S}^N}](\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N})\cdot|\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\right)\ .$$

satisfait (A.1), ce qui complète la preuve. □

Lemme A.1.2. *Le protocole de la figure 4.1 satisfait le deuxième critère de la définition 4.3.1.*

Démonstration. On doit argumenter que pour tout $\epsilon>0$, $\left\|\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N})\right\|_1\leq\exp(-\Omega(N))$ dès que $F(\theta_{\mathsf{S}},\varphi_{\mathsf{S}})^2<1-\epsilon$, où

$$\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}):=\mathrm{tr}_{\bar{\mathsf{R}}}\left(\langle\varphi|^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\cdot[\bar{U}_{\mathsf{P}^N}\otimes V^{[k]}_{\mathsf{S}^N}](\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N})\cdot|\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\right)\ .$$

La preuve est fondée sur le fait que la probabilité maximale d'observer $|\varphi\rangle^{\otimes k}$ en mesurant les registres $\mathsf{P}^k\mathsf{S}^k$ est égale à la fidélité (au carré) avec $\varphi^{\otimes k}$. Puisque la fidélité est multiplicative pour les états en produit tensoriel, il en découle que

$$\left\|\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}\left(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N}\right)\right\|_1\leq F(\theta^{\otimes k}_{\mathsf{S}^k},\varphi^{\otimes k}_{\mathsf{S}^k})^2\leq(1-\epsilon)^{2k}\leq\exp(-2\epsilon k)$$

dès que $F(\theta_{\mathsf{S}},\varphi_{\mathsf{S}})^2<1-\epsilon$ □

Le troisième critère de la définition 4.3.1 découle directement de l'observation que ni $\mathcal{E}^{\mathrm{acc}}_{\mathsf{R}\mathsf{S}^N\to\mathsf{S}^n}$ ni $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ n'agissent sur les registres non échantillonnés de S^N autre qu'en les permutant.

Lemme A.1.3. *Le protocole de la figure 4.1 satisfait le troisième critère de la définition 4.3.1.*

Démonstration. On doit montrer que le CPTN $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ définit dans le lemme A.1.1 satisfait la relation

$$\operatorname{tr}_\Pi\left(\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}})\right)\leq\theta^{\otimes n}_{\mathsf{S}}\quad.$$

Cette relation découle directement de la définition de $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$:

$$\begin{aligned}\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}}) &= \operatorname{tr}_{\bar{\mathsf{R}}}\left(\langle\varphi|^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\cdot[\bar{U}_{\mathsf{P}^N}\otimes V^{[k]}_{\mathsf{S}^N}](|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}})\cdot|\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\right)\\ &= \operatorname{tr}_{\bar{\mathsf{R}}}\left(\langle\varphi|^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\cdot[\bar{U}_{\mathsf{P}^N}\otimes \mathbb{1}_{\mathsf{S}^N}](|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}})\cdot|\varphi\rangle^{\otimes k}_{\mathsf{P}^k\mathsf{S}^k}\right)\\ &\leq\theta^{\otimes n}_{\mathsf{S}}\end{aligned}$$

où la deuxième égalité ci-dessus découle du fait que $|\theta\rangle\langle\theta|^{\otimes N}$ est invariant sous les permutations, donc $V^{[k]}_{\mathsf{S}^N}$ agit comme l'identité et l'inégalité est une conséquence de la remarque 2.9.1. □

A.2 Preuve de la proposition 4.3.2

Comme dans la section A.1, établissons que le protocole satisfait chacun des critères de la définition 4.3.1.

Lemme A.2.1 (Premier critère)**.** *Soit $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$ la sortie du protocole d'échantillonnage de la figure 4.3. Pour tout $\rho_{\mathsf{RS}^N}\in\mathcal{D}(\mathcal{H}_{\mathsf{R}}\otimes\mathcal{H}^{\otimes N}_{\mathsf{S}})$, il existe $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ tel que*

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n}|\pi\rangle\langle\pi|_\Pi\otimes\pi_{\mathsf{S}^n}\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N})\pi^*_{\mathsf{S}^n}=\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N})\tag{A.2}$$

pour une purification symétrique $|\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}\rangle$ de $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N}\pi_{\mathsf{S}^N}\rho_{\mathsf{S}^N}\pi^*_{\mathsf{S}^N}$.

Démonstration. Nous réutiliserons l'isométrie $V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}$ de la section A.1 qui, pour $t\subset[N]$, envoie les registres échantillonnés S_t dans les dernières k positions S^k et les registres non échantillonnés $S_{\bar{t}}$ dans les n premières positions S^n. Le CPTN $\mathcal{E}^{\text{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$ qui représente la sortie du protocole sur état d'entrée ρ_{RS^N} est décrit par

$$2^{-k}\binom{N}{k}^{-1}\sum_{t,c,x}\operatorname{tr}_{RS^k}\left((E^{t,c}_x\otimes\mathbb{P}^{x,c}_{\mathsf{S}^k})V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}\rho_{\mathsf{RS}^N}V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}\right)$$

où la somme est sur les sous-ensembles $t\subset[N]$ de taille k, sur les bases $c\in\{0,1\}^k$ et sur les chaines $x\in\{0,1\}^k$, et où $E^{t,c}=\{E^{t,c}_x\}_{x\in\{0,1\}^k}$ est la mesure POVM sur R qui produit x effectuée par Paul lorsque Sam lui envoie t et c et $\mathbb{P}^{x,c}_{\mathsf{S}^k}:=H^{\otimes c}|x\rangle\langle x|H^{\otimes c}$ est le projecteur sur l'état de base x pour la base c.

Soit $\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}$ une purification arbitraire de $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N}\pi_{\mathsf{S}^N}\rho_{\mathsf{S}^N}\pi^*_{\mathsf{S}^N}$. Définissons le super-opérateur $\bar{\mathcal{E}}^{\text{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ comme suit :

1. Transformer l'état $\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}$ en $\frac{1}{N!}\sum_{\pi\in\mathcal{S}_N}|\pi\rangle\langle\pi|_{\bar{\Pi}}\otimes(\mathbb{1}_{\mathsf{R}}\otimes\pi_{\mathsf{S}^N})\rho_{\mathsf{RS}^N}(\mathbb{1}_{\mathsf{R}}\otimes\pi^*_{\mathsf{S}^N})$.
2. Lire la permutation $\pi\in\mathcal{S}_N$ contenue dans le registre R et calculer t_π, $\tau^\pi\in\mathcal{S}_k$ et $\bar{\tau}^\pi\in\mathcal{S}_n$ tels que définis dans la remarque A.1.1.
3. Appliquer la transformation $V^{[k]}_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}$ sur les registres S^N, choisir $c\in\{0,1\}^k$ aléatoirement et appliquer la mesure POVM $E^{t_\pi,c}$ sur le registre R produisant le résultat x.
4. Mesurer les registres échantillonnés S^k en projetant sur l'état $H^{\otimes\tau^\pi(c)}|\tau^\pi(x)\rangle_{\mathsf{S}^k}=\tau^\pi H^{\otimes c}|x\rangle_{\mathsf{S}^k}$.
5. Produire une sortie composée de $\bar{\tau}^\pi$ dans le registre Π et des registres S^n.

La sortie de $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ sur entrée $\bar{\rho}_{\mathsf{P}^N\mathsf{S}^N}$ est

$$\begin{aligned}
&\frac{2^{-k}}{N!}\sum_{\pi,c,x}\mathrm{tr}_{\mathsf{RS}^k}\left((E^{t_\pi,c}_x\otimes\tau^\pi_{\mathsf{S}^k}\mathbb{P}^{x,c}_{\mathsf{S}^k}(\tau^\pi_{\mathsf{S}^k})^*)\cdot[V^{[k]}_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}\pi_{\mathsf{S}^N}](\rho_{\mathsf{RS}^N})\right)\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi\\
&=\frac{2^{-k}}{N!}\sum_{\pi,c,x}\bar{\tau}^\pi_{\mathsf{S}^n}\,\mathrm{tr}_{\mathsf{RS}^k}\left((E^{t_\pi,c}_x\otimes\mathbb{P}^{x,c}_{\mathsf{S}^k})[V^{t_\pi}_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}](\rho_{\mathsf{RS}^N})\right)\bar{\tau}^\pi_{\mathsf{S}^n}\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi\\
&=\frac{2^{-k}}{n!}\binom{N}{k}^{-1}\sum_{\bar{\tau}^\pi\in\mathcal{S}_n}[\bar{\tau}^\pi_{\mathsf{S}^n}]\left(\sum_{t,c,x}\mathrm{tr}_{\mathsf{RS}^k}\left((E^{t,c}_x\otimes\mathbb{P}^{x,c}_{\mathsf{S}^k})[V^t_{\mathsf{S}^N}](\rho_{\mathsf{RS}^N})\right)\right)\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi\\
&=\frac{1}{n!}\sum_{\bar{\tau}^\pi\in\mathcal{S}_n}\bar{\tau}^\pi_{\mathsf{S}^n}\mathcal{E}^{\mathrm{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}(\rho_{\mathsf{RS}^N})\bar{\tau}^\pi_{\mathsf{S}^n}\otimes|\bar{\tau}^\pi\rangle\langle\bar{\tau}^\pi|_\Pi
\end{aligned}$$

où la deuxième égalité ci-dessus utilise la remarque A.1.1. □

Lemme A.2.2 (Deuxième critère)**.** *Soit $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ tel que défini dans la preuve du lemme A.2.1. Pour tout $\epsilon>0$, $\|\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N})\|_1\leq\exp(-\Omega(N))$ dès que $F(\theta_{\mathsf{S}},\varphi_{\mathsf{S}})^2<1-\epsilon$*

Démonstration. Pour tout $c\in\{0,1\}^k$, soit $\bar{E}^c_x$ l'élément de POVM qui, lorsqu'appliqué sur P^N, donne la probabilité que x soit produit à l'étape 3 de $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ lorsque c est choisi à la même étape. En d'autres termes, $\bar{E}^c_x$ est à $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ ce que $E^{t_\pi,c}$ est à $\mathcal{E}^{\mathrm{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$; il donne la probabilité d'observer x lorsque la mesure suivante est faite sur les registres P^N : produire les registres $\bar{\Pi}\mathsf{R}$ à partir de P^N, mesurer π du registre $\bar{\Pi}$, calculer l'échantillon correspondant t_π, et appliquer la mesure POVM $E^{t_\pi,c}$.

En utilisant ces opérateurs de POVM $\bar{E}^c_x$, on peut exprimer la norme qu'on veut borner supérieurement comme

$$\left\|\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N})\right\|_1=2^{-k}\sum_{c,x}\mathrm{tr}\left((\bar{E}^c_x\otimes\mathbb{P}^{x,c}_{\mathsf{S}^k}\otimes\mathbb{1}_{\mathsf{S}^n})|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{P}^N\mathsf{S}^N}\right)\tag{A.3}$$

où $\mathbb{P}^{x,c}_{\mathsf{S}^k}$ est le projecteur sur l'élément x de la base c. Notons que la partie droite de (A.3) peut être interprétée comme la probabilité de deviner le résultat de la mesure des registres S^k dans une base aléatoirement choisie, mais connue c en observant l'état réduit des registres P^N. Nous analysons maintenant cette probabilité de deviner x, afin d'obtenir une borne supérieure sur (A.3).

Puisque les opérateurs $\mathbb{P}_{\mathsf{S}^k}^{x,c}$ de la mesure projective faite sur S^k est sous forme de produit ($\mathbb{P}_{\mathsf{S}^k}^{x,c} = \bigotimes_{i=1}^{k} H^{\otimes c_i}|x_i\rangle\langle x_i|H^{\otimes c_i}$) et puisque l'état de $\mathsf{P}^k\mathsf{S}^k$ est sous une forme i.i.d., la probabilité de deviner la valeur que prend x à partir des registres P^N est de la forme γ^k où γ correspond à la probabilité de deviner un seul bit de x. Puisque les deux valeurs possibles pour la base sont équiprobables, cette probabilité est donnée par l'expression

$$\gamma = \frac{1}{2}\Pr(\text{deviner } X \,:\, C=0) + \frac{1}{2}\Pr(\text{deviner } X \,:\, C=1) \tag{A.4}$$

où X est la variable aléatoire correspondant du résultat de la mesure de θ_{S} dans la base C.

Montrons maintenant qu'au moins un des deux termes de (A.4) est borné supérieurement par une constante strictement plus petite que 1 lorsque $F(\theta_{\mathsf{S}}, \varphi_{\mathsf{S}}) < 1-\epsilon$, ce qui implique que γ^k est négligeable en k. La probabilité maximale de deviner X lorsque $C=0$ est donnée par la probabilité maximale de distinguer les états réduits

$$\left|\theta_{\mathsf{P}}^0\right\rangle = (\mathbb{1}_{\mathsf{P}} \otimes \langle 0|_{\mathsf{S}})|\theta_{\mathsf{PS}}\rangle \text{ and } \left|\theta_{\mathsf{P}}^1\right\rangle = (\mathbb{1}_{\mathsf{P}} \otimes \langle 1|_{\mathsf{S}})|\theta_{\mathsf{PS}}\rangle$$

et de même lorsque $C=1$ pour les états $|\theta_{\mathsf{P}}^+\rangle$ et $|\theta_{\mathsf{P}}^-\rangle$ définis de manière similaire. Soit

$$\sqrt{\lambda_0}|f_0\rangle_{\mathsf{P}}|e_0\rangle_{\mathsf{S}} + \sqrt{\lambda_1}|f_1\rangle_{\mathsf{P}}|e_1\rangle_{\mathsf{S}}$$

la forme de Schmidt de $|\theta_{\mathsf{PS}}\rangle$ et considérons la quantité

$$\begin{aligned}
&\left|\langle\theta_{\mathsf{P}}^0|\theta_{\mathsf{P}}^1\rangle\right| + \left|\langle\theta_{\mathsf{P}}^+|\theta_{\mathsf{P}}^-\rangle\right| \geq \left|\langle\theta_{\mathsf{P}}^0|\theta_{\mathsf{P}}^1\rangle + \langle\theta_{\mathsf{P}}^+|\theta_{\mathsf{P}}^-\rangle\right| \\
&= |\langle\theta_{\mathsf{PS}}|(\mathbb{1}_{\mathsf{P}} \otimes |0\rangle\langle 1|_{\mathsf{S}})|\theta_{\mathsf{PS}}\rangle + \langle\theta_{\mathsf{PS}}|(\mathbb{1}_{\mathsf{P}} \otimes |+\rangle\langle -|_{\mathsf{S}})|\theta_{\mathsf{PS}}\rangle| \\
&= \frac{1}{\sqrt{2}}\,|\langle\theta_{\mathsf{PS}}|(\mathbb{1}_{\mathsf{P}} \otimes H_{\mathsf{S}})|\theta_{\mathsf{PS}}\rangle| = \frac{1}{\sqrt{2}}\,|\lambda_0\langle e_0|_{\mathsf{S}}H_{\mathsf{S}}|e_0\rangle_{\mathsf{S}} + \lambda_1\langle e_1|_{\mathsf{S}}H_{\mathsf{S}}|e_1\rangle_{\mathsf{S}}| \\
&= \frac{1}{\sqrt{2}}\,|\lambda_0 - \lambda_1|
\end{aligned}$$

où H est la transformation de Hadamard. La seule inégalité ci-dessus est l'inégalité du triangle et la dernière égalité découle du fait que $\langle e_0|_{\mathsf{S}}H|e_0\rangle = -\langle e_1|H|e_1\rangle$ pour n'importe quels deux vecteurs orthogonaux $|e_0\rangle$ et $|e_1\rangle$. Le dernier terme de l'équation ci-dessus peut être borné supérieurement par ϵ puisque

$$|\lambda_0 - \lambda_1| = \left|\lambda_0 - \frac{1}{2}\right| + \left|\lambda_1 - \frac{1}{2}\right| = \left\|\theta_{\mathsf{S}} - \frac{\mathbb{1}_{\mathsf{S}}}{2}\right\|_1 \geq 2(1 - F(\theta_{\mathsf{S}}, \frac{\mathbb{1}_{\mathsf{S}}}{2})) \geq 2\epsilon \ .$$

Supposons que $\left|\langle\theta_{\mathsf{P}}^0|\theta_{\mathsf{P}}^1\rangle\right| \geq \epsilon/2$ (sinon, $\left|\langle\theta_{\mathsf{P}}^+|\theta_{\mathsf{P}}^-\rangle\right| \geq \epsilon/2$ et le même argument tient pour ces deux états). Ceci veut dire que Paul ne peut pas distinguer entre les deux états réduits $|\theta_{\mathsf{P}}^0\rangle$ et $|\theta_{\mathsf{P}}^1\rangle$ avec probabilité meilleure que $1-f(\epsilon)$, où f est une fonction croissante, par le théorème d'Helström. On peut donc conclure que γ est borné supérieurement pas une constante strictement plus petite que 1 et que la probabilité γ^k de deviner le résultat de mesure pour toutes les positions est négligeable en k. □

Le troisième critère de la définition 4.3.1 découle directement de l'observation que ni $\mathcal{E}^{\mathrm{acc}}_{\mathsf{RS}^N\to\mathsf{S}^n}$ ni $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ n'agit sur les registres non échantillonnés autrement que par une permutation de ceux-ci.

Lemme A.2.3. *Le protocole de la figure 4.3 satisfait le troisième critère de la définition 4.3.1.*

Démonstration. On doit montrer que le CPTN $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$ définit dans le lemme A.2.1 satisfait la relation

$$\mathrm{tr}_\Pi\left(\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}})\right)\leq\theta^{\otimes n}_{\mathsf{S}}\ .$$

Cette relation découle directement de la définition de $\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}$:

$$\begin{aligned}\bar{\mathcal{E}}^{\mathrm{acc}}_{\mathsf{P}^N\mathsf{S}^N\to\Pi\mathsf{S}^n}(|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}}) &= 2^{-k}\binom{N}{k}^{-1}\sum_{t,c,x}\mathrm{tr}_{RS^k}\left((E^{t,c}_x\otimes\mathbb{P}^{x,c}_{\mathsf{S}^k})V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}}V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}\right)\\ &= 2^{-k}\binom{N}{k}^{-1}\sum_{t,c,x}\mathrm{tr}_{RS^k}\left((E^{t,c}_x\otimes\mathbb{P}^{x,c}_{\mathsf{S}^k})|\theta\rangle\langle\theta|^{\otimes N}_{\mathsf{PS}}\right)\\ &\leq\theta^{\otimes n}_{\mathsf{S}}\end{aligned}$$

où la deuxième égalité ci-dessus découle du fait que $|\theta\rangle\langle\theta|^{\otimes N}$ est invariant sous les permutations, donc $V^t_{\mathsf{S}^N\to\mathsf{S}^n\mathsf{S}^k}$ agit comme l'identité et l'inégalité est une conséquence de la remarque 2.9.1. □